SonicWALL Network Security Appliances

NETWORK SECURITY

NSA 240

Getting Started Guide

SONICWALL®

SonicWALL NSA 240 Getting Started Guide

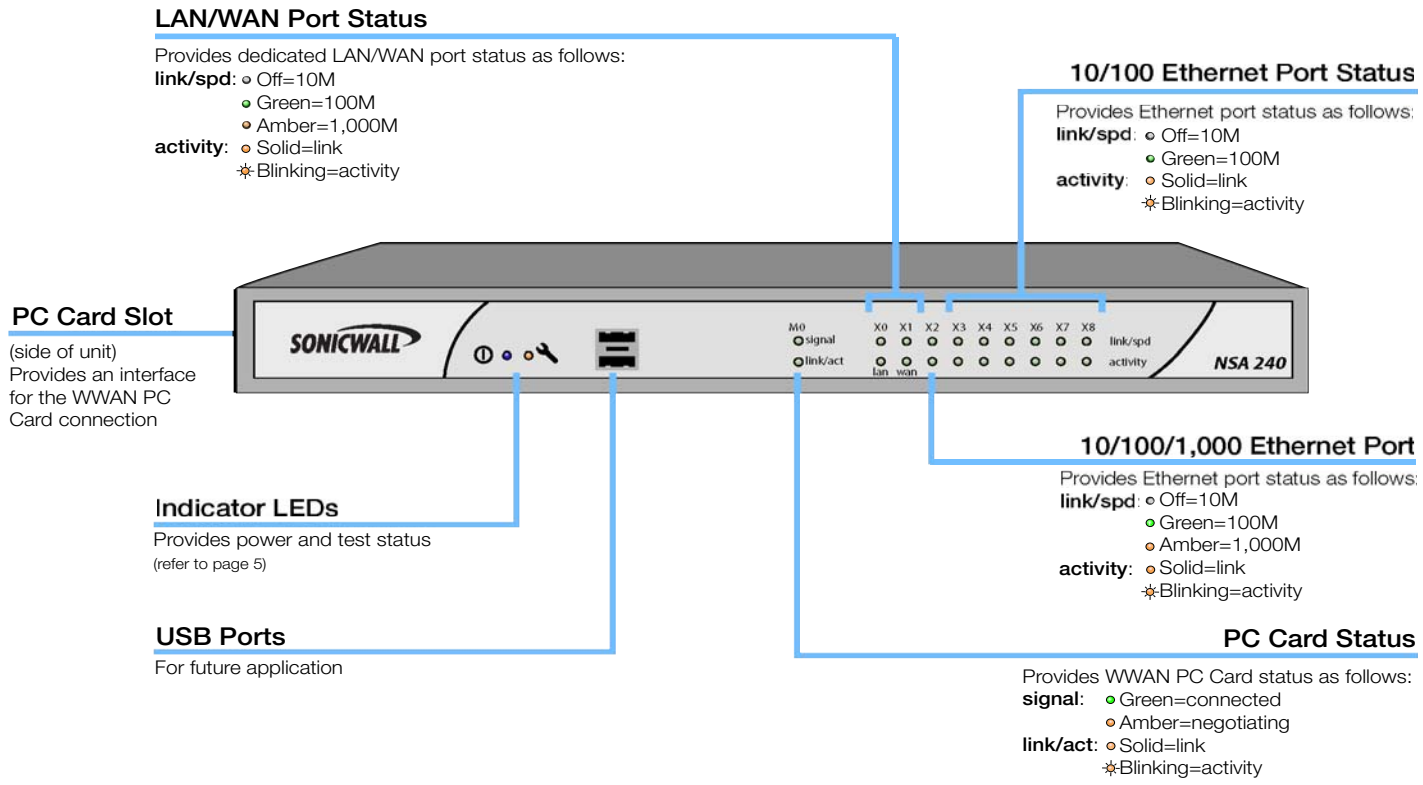
This *Getting Started Guide* provides instructions for basic installation and configuration of the SonicWALL Network Security Appliance (NSA) 240 running SonicOS Enhanced. After you complete this guide, computers on your Local Area Network (LAN) will have secure Internet access.

Document Contents

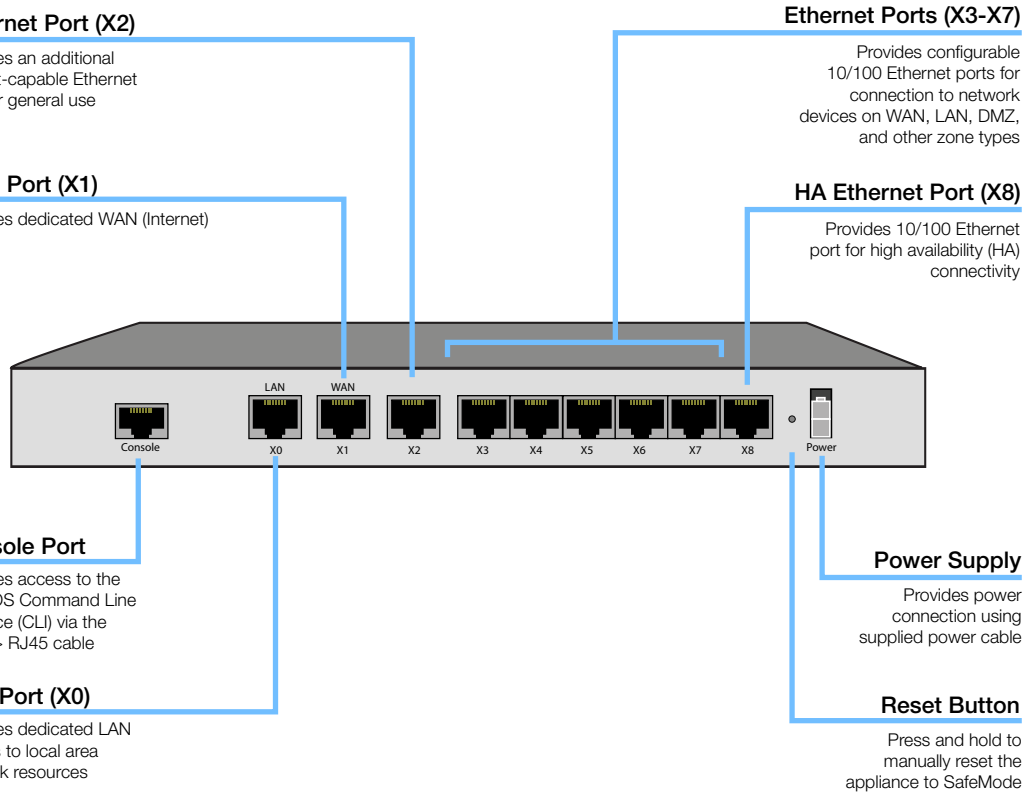
This document contains the following sections:

1. *Pre-Configuration Tasks - page 1*
2. *Preparing Your WWAN PC Card - page 7*
3. *Registering Your Appliance - page 11*
4. *Deployment Scenarios - page 17*
5. *Verifying Your Connection - page 35*
6. *Enabling Essential Security Services - page 39*
7. *Additional Deployment Configuration - page 47*
8. *Support and Training Options - page 71*
9. *Product Safety and Regulatory Information - page 79*

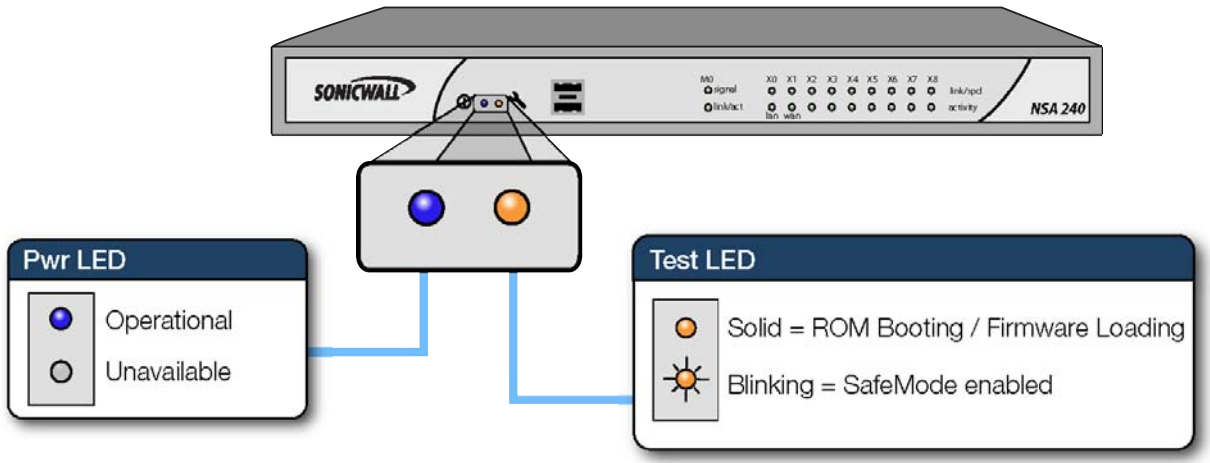
SonicWALL NSA 240 Front Panel



SonicWALL NSA 240 Rear Panel


Ethernet Port (X2)
Provides an additional Gigabit-capable Ethernet port for general use
Ethernet Ports (X3-X7)
Provides configurable 10/100 Ethernet ports for connection to network devices on WAN, LAN, DMZ, and other zone types
WAN Port (X1)
Provides dedicated WAN (Internet)
HA Ethernet Port (X8)
Provides 10/100 Ethernet port for high availability (HA) connectivity
LAN
WAN
Console
X0
X1
X2
X3
X4
X5
X6
X7
X8
Power
Console Port
Provides access to the SonicOS Command Line Interface (CLI) via the DB9 -> RJ45 cable
Power Supply
Provides power connection using supplied power cable
LAN Port (X0)
Provides dedicated LAN access to local area network resources
Reset Button
Press and hold to manually reset the appliance to SafeMode

SonicWALL NSA 240 LED Reference Guide



Pre-Configuration Tasks 1

In this Section:

This section provides pre-configuration information. Review this section before setting up your SonicWALL NSA 240 appliance.

- *Checking NSA 240 Package Contents* - page 2
- *Obtaining Configuration Information* - page 3
- *Obtaining WWAN Service Provider Information* - page 5
- *Verifying System Requirements* - page 6

Checking NSA 240 Package Contents

Before setting up your SonicWALL NSA appliance, verify that your package contains the following parts:

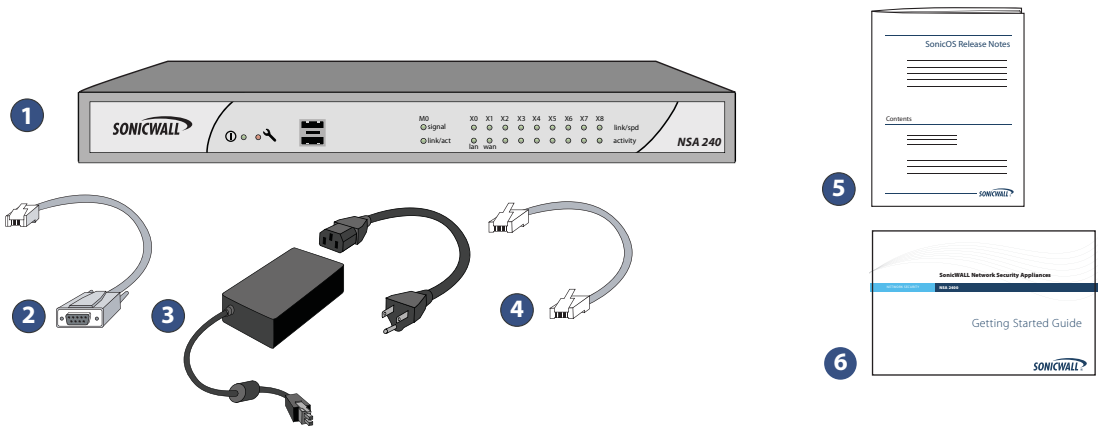
1. NSA 240 Appliance
2. DB9 -> RJ45 (CLI) Cable
3. Standard Power Adaptor*
4. Ethernet Cable
5. Release Notes
6. Getting Started Guide

Any Items Missing?

If any items are missing from your package, please **contact SonicWALL support**.

A listing of the most current support documents are available online at: <http://www.sonicwall.com/us/support.html>

*The included power cord is intended for use in North America only. For European Union (EU) customers, a power cord is not included.



Obtaining Configuration Information

Record and keep for future reference the following setup information:

Registration Information

Serial Number:	Record the serial number found on the bottom panel of your SonicWALL appliance.
Authentication Code:	Record the authentication code found on the bottom panel of your SonicWALL appliance.

Networking Information

LAN IP Address: _____._____._____._____	Select a static IP address for your SonicWALL appliance that is within the range of your local subnet. If you are unsure, you can use the default IP address (192.168.168.168).
Subnet Mask: _____._____._____._____	Record the subnet mask for the local subnet where you are installing your SonicWALL appliance.
Ethernet WAN IP Address: _____._____._____._____	Select a static IP address for your Ethernet WAN. *This setting only applies if you are already using an ISP that assigns a static IP address.*

Administrator Information

Admin Name:	Select an administrator account name. (default is *admin)*
Admin Password:	Select an administrator password. (default is *password*)

Obtaining Internet Service Provider (ISP) Information

Record the following information about your current ISP:

ISP 1

If you connect via	You likely use	Please record
Cable modem, DSL with a router	DHCP	*No Internet connection information is usually required*, although some service providers require a host name. Host Name: _____
Home DSL	PPPoE	User Name: _____ Password: _____ *Note: Your ISP may require your user name in the format: name@ISP.com*
T1/E1, Static broadband, Cable or DSL with a static IP	Static IP	IP Address: _____._____._____._____ Subnet Mask: _____._____._____._____ Default Gateway (IP Address): _____._____._____._____ Primary DNS: _____._____._____._____ Secondary DNS (optional): _____._____._____._____
Dial-in to a server	PPTP	Server Address: _____ User Name: _____ Password: _____

Record the following information about your secondary ISP:

ISP 2 (Optional for Multiple WAN Failover)

If you connect via	You likely use	Please record
Cable modem, DSL with a router	DHCP	Host Name: _____
Home DSL	PPPoE	User Name: _____ Password: _____ *Note: Your ISP may require your user name in the format: name@ISP.com*
T1/E1, Static broadband, Cable or DSL with a static IP	Static IP	IP Address: _____._____._____._____ Subnet Mask: _____._____._____._____ Default Gateway (IP Address): _____._____._____._____ Primary DNS: _____._____._____._____ Secondary DNS (optional): _____._____._____._____
Dial-in to a server	PPTP	Server Address: _____ User Name: _____ Password: _____

Obtaining WWAN Service Provider Information

Record the following information about your current WWAN service:

WWAN Service Provider

Country:	Record the country where you purchased your WWAN card.
Service Provider:	Record the service provider from whom you purchased your WWAN card. This is the brand name of the card.
Plan Type:	Record the plan type that you purchased from your provider. If you are unsure about this information, you may use **Standard** as the plan type.

WWAN Account Information

User Name/Password:	Some WWAN service providers require user specific information, such as a login and password. If your service provider requires it, you will need to provide such information during the setup process.

Note: ***WWAN Account Information*** *is automatically populated based on the chosen service provider and plan type. In most cases, if you selected the correct service provider and plan type the WWAN account information does not have to be altered.*

Verifying System Requirements

Before you begin the setup process, verify that you have:

- An Internet connection
- A Web browser supporting Java Script and HTTP uploads. Supported browsers include the following:

	Supported Browsers	Browser Version Number
	Internet Explorer	6.0 or higher
	Firefox	2.0 or higher
	Netscape	9.0 or higher
	Opera	9.10 or higher for Windows
	Safari	2.0 or higher for MacOS

Preparing Your WWAN PC Card 2

In this Section:

This section provides instructions to set up your WWAN PC card for use in the SonicWALL NSA 240 appliance.

- *WWAN PC Card Setup* - page 8
- *Activating Your PC Card Software* - page 8
- *Verifying Your Connection* - page 9

Alert: *DO NOT insert your PC card into the SonicWALL NSA 240 appliance until you have completed the setup process for your card as described in this section.*

If your WWAN PC card is already registered and activated with your service provider and you are able to access the Internet through your PC using this card, you may skip this section and continue to *Registering Your Appliance - page 11*.

WWAN PC Card Setup

Complete the following steps to set up and provision your WWAN PC card. Verify at the www.sonicwall.com website that your WWAN PC card and service provider are supported by the SonicWALL NSA 240 appliance.

Alert: *DO NOT insert your PC card into the SonicWALL NSA 240 appliance until you have completed the setup process for your card as described in this section and successfully accessed the Internet through your computer using the PC card.*

If you are using a GSM-based WWAN service provider, you may be required to remove the PIN protection from your SIM chip before using it with the SonicWALL. Please contact your WWAN service provider for more information on setup and PIN removal procedures.

Activating Your PC Card Software

This section covers prerequisites necessary to set up most WWAN PC cards to work with the SonicWALL NSA 240. Using an available desktop or laptop PC with Type II PC card slot, complete the following steps:

1. Install the software that came bundled with your WWAN PC card before activating the card.
2. When prompted, insert the WWAN PC card into an available Type II PC card slot on the Laptop or Desktop PC you are using for card configuration.
3. Install updates to your WWAN PC card, if available.
4. Activate your PC card, if required.

Verifying Your Connection

After activating the card on your PC, you can view your connection type and verify that the WWAN PC card is transferring data. For valid connection testing, it is important that you first disable all other network connections, such as a WiFi or LAN connection, before continuing. Leave only your PC card connection enabled.

1. Use the software that came with your WWAN PC card to initialize a connection with your service provider.
2. In the Windows interface, select **Start > Run**.
3. Enter **cmd** in the Open field and click the **OK** button.
4. At the prompt, type the command **ipconfig** and press **Enter** on the keyboard.
5. Your network device status will display. Verify that you have obtained an IP Address for your Ethernet adaptor, and that all other Local Area Network Connections display “Media disconnected” as their status.

Note: *The name of your **Ethernet adaptor** may differ from the screenshot below. Common names for newly acquired cards are “Local Area Connection 2” or “Local Area Connection 3.”*

C:\Documents and Settings\pmlydon>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Media State . . . . . : Media disconnected
Ethernet adapter Local Area Connection 2:
Connection-specific DNS Suffix . :
IP Address. . . . . : 166.214.210.64
Subnet Mask . . . . . : 255.255.255.255
Default Gateway . . . . . : 166.214.210.64

6. Open a Web browser and navigate to a Website, such as <*http://www.sonicwall.com*>, to verify that your connection can transfer data.

Congratulations! You have set up and provisioned your WWAN PC card.

Registering Your Appliance 3

In this Section:

This section provides instructions for registering your SonicWALL NSA 240 appliance.

- *Before You Register - page 12*
- *Creating a MySonicWALL Account - page 13*
- *Registering and Licensing Your Appliance on MySonicWALL - page 13*

Note: *Registration is an important part of the setup process and is necessary to receive the benefits of SonicWALL security services, firmware updates, and technical support.*

Before You Register

You need a MySonicWALL account to register the SonicWALL NSA appliance. You can create a new MySonicWALL account on www.mysonicwall.com or directly from the SonicWALL management interface. This section describes how to create an account by using the Website.

If you already have a MySonicWALL account, go to *Registering and Licensing Your Appliance on MySonicWALL - page 13* to register your appliance on MySonicWALL. You can also postpone registration until after you set up the appliance. Skip ahead to *Deployment Scenarios - page 17* and register your appliance directly from the management interface once you reach *Activating Licenses in SonicOS* - page 40.

For a High Availability (HA) configuration, you must use MySonicWALL to associate a backup unit that can share the Security Services licenses with your primary SonicWALL.

If you do not yet have a MySonicWALL account, you can use MySonicWALL to register your SonicWALL appliance and activate or purchase licenses for Security Services, ViewPoint Reporting and other services, support, or software before you even connect your device. This method allows you to prepare for your deployment before making any changes to your existing network.

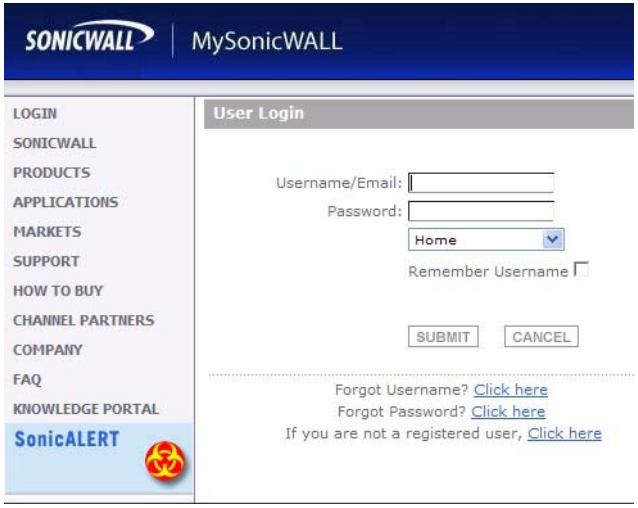
Note that your SonicWALL NSA appliance does not need to be powered on during account creation or during the registration and licensing process on mysonicwall.com.

Note: *After registering a new SonicWALL appliance on MySonicWALL, you must also register the appliance from the SonicOS management interface. This allows the unit to synchronize with the SonicWALL License Server and to share licenses with the associated appliance, if any. See Activating Licenses in SonicOS - page 40.*

Creating a MySonicWALL Account

To create a MySonicWALL account, perform the following steps:

1. In your browser, navigate to www.mysonicwall.com.
2. In the login screen, click the **If you are not a registered user, Click here** link.



3. Complete the Registration form and click **Register**.
4. Verify the information is correct and click **Submit**.
5. In the screen confirming that your account was created, click **Continue**.

Registering and Licensing Your Appliance on MySonicWALL

This section contains the following subsections:

- *Product Registration* - page 13
- *Licensing Security Services and Software* - page 14
- *Registering a Second Appliance as a Backup* - page 16

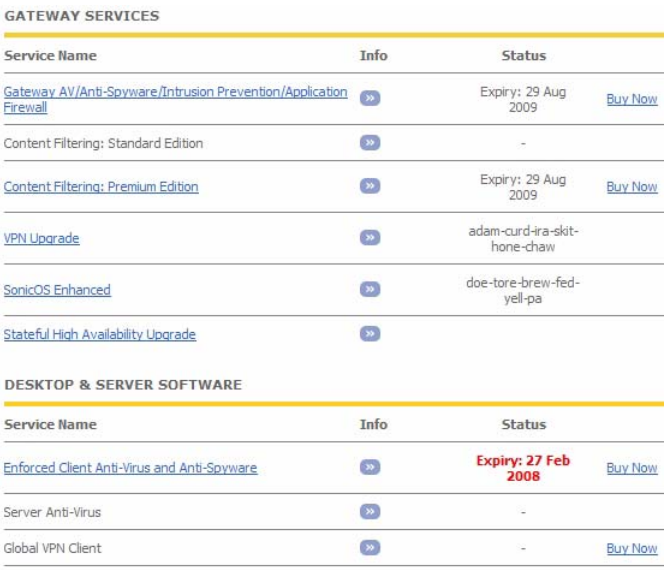
Product Registration

You must register your SonicWALL security appliance on MySonicWALL to enable full functionality.

1. Login to your MySonicWALL account. If you do not have an account, you can create one at www.mysonicwall.com.
2. On the main page, type the appliance serial number in the **Register A Product** field. Then click **Next**.
3. On the My Products page, under **Add New Product**, type the friendly name for the appliance, select the **Product Group** if any, type the authentication code into the appropriate text boxes, and then click **Register**.
4. On the Product Survey page, fill in the requested information and then click **Continue**.

Licensing Security Services and Software

The Service Management - Associated Products page in MySonicWALL lists security services, support options, and software, such as ViewPoint, that you can purchase or try with a free trial. For details, click the **Info** button. Your current licenses are indicated in the **Status** column with either a license key or an expiration date. You can purchase additional services now or at a later time.



GATEWAY SERVICES

Service Name	Info	Status	
Gateway AV/Anti-Spyware/Intrusion Prevention/Application Firewall	»	Expiry: 29 Aug 2009	Buy Now
Content Filtering: Standard Edition	»	-	
Content Filtering: Premium Edition	»	Expiry: 29 Aug 2009	Buy Now
VPN Upgrade	»	adam-curd-ira-skit-hone-chaw	
SonicOS Enhanced	»	doe-tore-brew-fed-yell-pa	
Stateful High Availability Upgrade	»		

DESKTOP & SERVER SOFTWARE

Service Name	Info	Status	
Enforced Client Anti-Virus and Anti-Spyware	»	Expiry: 27 Feb 2008	Buy Now
Server Anti-Virus	»	-	
Global VPN Client	»	-	Buy Now

The following products and services are available for the SonicWALL NSA 240:

- **Service Bundles:**
  - Client/Server Anti-Virus Suite
  - Comprehensive Gateway Security Suite
- **Gateway Services:**
  - Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, Application Firewall
  - Global Management System
  - Content Filtering: Premium Edition
  - Stateful High Availability Upgrade
- **Desktop and Server Software:**
  - Enforced Client Anti-Virus and Anti-Spyware
  - Global VPN Client
  - Global VPN Client Enterprise
  - ViewPoint
- **Support Services:**
  - Dynamic Support 8x5
  - Dynamic Support 24x7
  - Software and Firmware Updates

To manage your licenses, perform the following tasks:

1. Navigate to the **My Products** page. Select the registered product you want to manage. Your initial purchase may have included security services or other software bundled with the appliance. These licenses are enabled on MySonicWALL when the SonicWALL appliance is delivered to you.
2. If you purchase a service subscription or upgrade from a sales representative separately, you will receive an **Activation Key** for the product. This key is emailed to you after online purchases, or is on the front of the certificate that was included with your purchase. Locate the product on the Service Management page and click **Enter Key** in that row.
3. In the Activate Service page, type or paste your key into the **Activation Key** field and then click **Submit**. Depending on the product, you will see an expiration date or a license key string in the **Status** column when you return to the Service Management page.
4. To license a product or service, do one of the following:
   - To try a Free Trial of a service, click **Try** in the Service Management page. A 30-day free trial is immediately activated. The Status page displays relevant information including the activation status, expiration date, number of licenses, and links to installation instructions or other documentation. The Service Management page is also updated to show the status of the free trial.
   - To purchase a product or service, click **Buy Now**.
5. In the Buy Service page, type the number of licenses you want in the **Quantity** column for either the 1-year, 2-year, or 3-year license row and then click **Add to Cart.**
6. In the Checkout page, follow the instructions to complete your purchase.

The MySonicWALL server will generate a license key for the product. The key is added to the license keyset. You can use the license keyset to manually apply all active licenses to your SonicWALL appliance.

The service management screen will display the product you licensed with an expiration date when activation is complete.

Registering a Second Appliance as a Backup

To ensure that your network stays protected if your SonicWALL appliance has an unexpected failure, you can purchase a license to associate a second SonicWALL of the same model as the first in a High Availability (HA) pair. After registering and associating the second appliance, this appliance will automatically share the Security Services licenses of the primary appliance.

To register a second appliance and associate it with the primary, perform the following steps:

1. Login to your MySonicWALL account.
2. On the main page, in the Register A Product field, type the appliance serial number and then click **Next**.
3. On the My Products page, under Add New Product, type the friendly name for the appliance, select the Product Group if any, type the authentication code into the appropriate text boxes, and then click **Register**.
4. On the Product Survey page, fill in the requested information and then click **Continue**. The Create Association Page is displayed.
5. On the Create Association Page, click the radio button to select the primary unit for this association, and then click **Continue**. The screen only displays units that are not already associated with other appliances.
6. On the Service Management - Associated Products page, scroll down to the Associated Products section to verify that your product registered successfully. You should see the HA Primary unit listed in the Parent Product section, as well as a Status value of **0** in the Associated Products / Child Product Type section.
7. Although the Stateful High Availability Upgrade and all the Security Services licenses can be shared with the HA Primary unit, you must purchase a separate ViewPoint license for the backup unit. This will ensure that you do not miss any reporting data in the event of a failover. Under Desktop & Server Software, click **Buy Now** for ViewPoint. Follow the instructions to complete the purchase.

To return to the Service Management - Associated Products page, click the serial number link for this appliance.

For information on configuring an HA pair, see *Scenario B: HA Pair in NAT/Route Mode* section, on page 24.

Deployment Scenarios 4

In this Section:

This section provides detailed overviews of advanced deployment scenarios as well as configuration instructions for connecting your SonicWALL NSA 240.

- *Initializing the SonicWALL* - page 18
- *Selecting a Deployment Scenario* - page 19
  - *Scenario A: NAT/Route Mode Gateway* - page 20
  - *Scenario B: HA Pair in NAT/Route Mode* - page 24
  - *Scenario C: L2 Bridge Mode* - page 31

Tip: *Before completing this section, fill out the information in Obtaining Configuration Information - page 3. You will need to enter this information during the **Setup Wizard**.*

Initializing the SonicWALL

To begin deployment of your SonicWALL NSA 240 appliance, first insert the WWAN PC card and then apply power to the appliance.

Inserting the WWAN PC Card

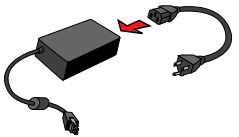
Before inserting the WWAN PC card into your SonicWALL NSA 240 appliance, be sure your WWAN PC card is activated and unlocked. If you are not sure whether your card is unlocked or not, contact the PC card vendor to verify.

Alert: *Do not insert or remove the WWAN PC card while the SonicWALL NSA 240 is powered on.*

1. Ensure that the SonicWALL NSA 240 is **not** connected to a power source.
2. Insert your WWAN PC card “face up” into the PC CARD slot on the left side of the SonicWALL NSA 240 appliance. The card should sit firmly in place.

Applying Power

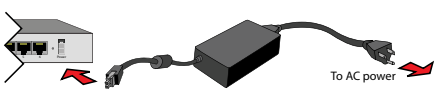
1. Connect the AC plug to the power supply.



2. Plug one end of the power supply to the back of the SonicWALL NSA 240.

Warning: *SonicWALL power supplies are platform specific. Do not use power supplies from other SonicWALL platforms, such as the SonicWALL TZ 190.*

3. *Connect the AC plug to an appropriate power outlet.*



The Power LED on the front panel lights up blue when you plug in the SonicWALL NSA. The Test LED will light up and may blink while the appliance performs a series of diagnostic tests.

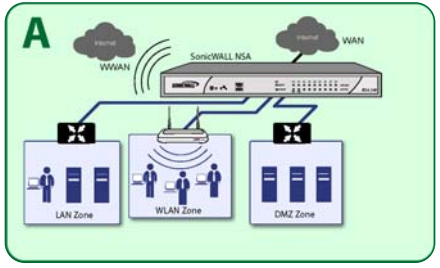
When the Power LED is lit and the Test LED is no longer lit, the SonicWALL NSA 240 is ready for configuration. This typically occurs within a few minutes of applying power to the appliance. If the Test LED remains lit after the SonicWALL NSA appliance has been booted, restart the appliance by cycling power.

Selecting a Deployment Scenario

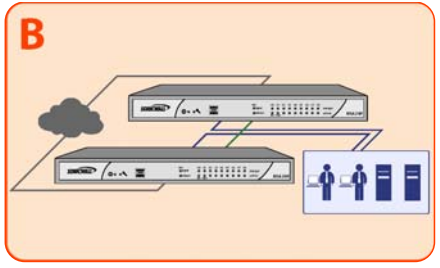
Before continuing, select a deployment scenario that best fits your network scheme. Reference the table below and the diagrams on the following pages for help in choosing a scenario.

Current Gateway Configuration	New Gateway Configuration	Use Scenario
No gateway appliance	Single SonicWALL NSA as a primary gateway.	**A** - NAT/Route Mode Gateway
	Pair of SonicWALL NSA appliances for high availability.	**B** - NAT with HA Pair
Existing Internet gateway appliance	SonicWALL NSA as replacement for an existing gateway appliance.	**A** - NAT/Route Mode Gateway
	SonicWALL NSA in addition to an existing gateway appliance.	**C** - Layer 2 Bridge Mode
Existing SonicWALL NSA 240 gateway appliance	SonicWALL NSA in addition to an existing SonicWALL NSA gateway appliance.	**B** - NAT with HA Pair

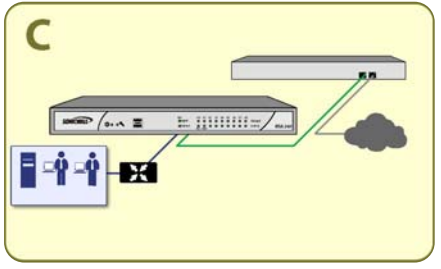
NAT/Route Mode Gateway



NAT with HA Pair

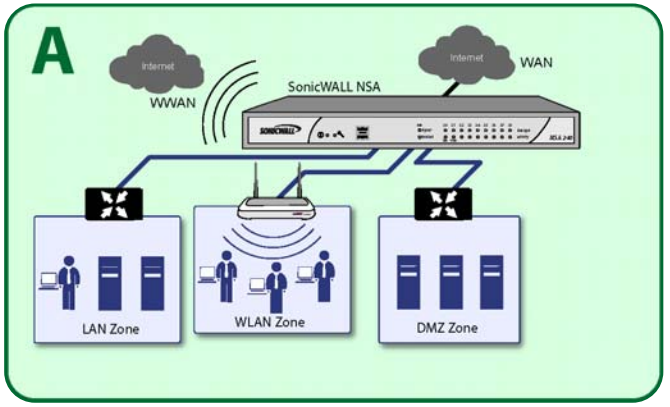


Layer 2 Bridge Mode



Scenario A: NAT/Route Mode Gateway

In this scenario, the SonicWALL NSA 240 is configured in NAT/Route mode to operate as a single network gateway. Two Internet sources may be routed through the SonicWALL appliance for load balancing and failover purposes. Because only a single SonicWALL appliance is deployed, the added benefits of high availability with a stateful synchronized pair are not available.



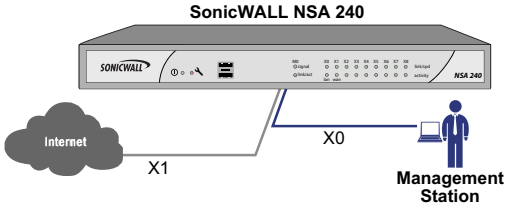
This section provides initial configuration instructions for connecting your SonicWALL NSA 240. Follow these steps if you are setting up **Scenario A**.

This section contains the following subsections:

- *Connecting the WAN Port* - page 21
- *Connecting the LAN Port* - page 21
- *Accessing the Management Interface* - page 21
- *Troubleshooting Initial Setup* - page 22
- *Connecting to Your Network* - page 23
- *Testing Your Connection* - page 23

Connecting the WAN Port

1. Connect one end of an Ethernet cable to your Internet connection.
2. Connect the other end of the cable to the **X1** (**WAN**) port on your SonicWALL NSA Series appliance.



Connecting the LAN Port

1. Connect one end of the provided Ethernet cable to the computer you are using to manage the SonicWALL NSA appliance.
2. Connect the other end of the cable to the **X0** port on your SonicWALL NSA appliance.

   The Link LED above the **X0** (**LAN**) port will light up in green or amber depending on the link throughput speed, indicating an active connection:

   - Amber indicates 1 Gbps
   - Green indicates 100 Mbps
   - Unlit while the right (activity) LED is illuminated indicates 10 Mbps

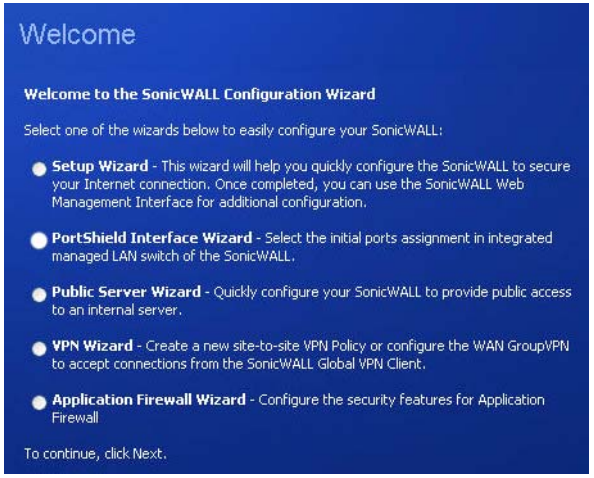
Accessing the Management Interface

The computer you use to manage the SonicWALL NSA Series must be set up to have an unused IP address on the 192.168.168.x/24 subnet, such as 192.168.168.20.

To access the SonicOS Enhanced Web-based management interface:

1. Start your Web browser. Remember to disable pop-up blocking software or add the management IP address http://192.168.168.168 to your pop-up blocker's allow list.
2. Enter **http://192.168.168.168** (the default LAN management IP address) in the **Location** or **Address** field.

3. The **SonicWALL Setup Wizard** launches and guides you through the configuration and setup of your SonicWALL NSA appliance.


Welcome
Welcome to the SonicWALL Configuration Wizard
Select one of the wizards below to easily configure your SonicWALL:
Setup Wizard - This wizard will help you quickly configure the SonicWALL to secure your Internet connection. Once completed, you can use the SonicWALL Web Management Interface for additional configuration.
PortShield Interface Wizard - Select the initial ports assignment in integrated managed LAN switch of the SonicWALL.
Public Server Wizard - Quickly configure your SonicWALL to provide public access to an internal server.
VPN Wizard - Create a new site-to-site VPN Policy or configure the WAN GroupVPN to accept connections from the SonicWALL Global VPN Client.
Application Firewall Wizard - Configure the security features for Application Firewall
To continue, click Next.

The **Setup Wizard** launches only upon initial loading of the SonicWALL NSA management interface. You may also access the wizard by clicking on the **Wizards** icon in the toolbar.

4. Follow the on-screen prompts to complete the Setup Wizard.
Depending on the changes made during your setup configuration, the SonicWALL may restart.

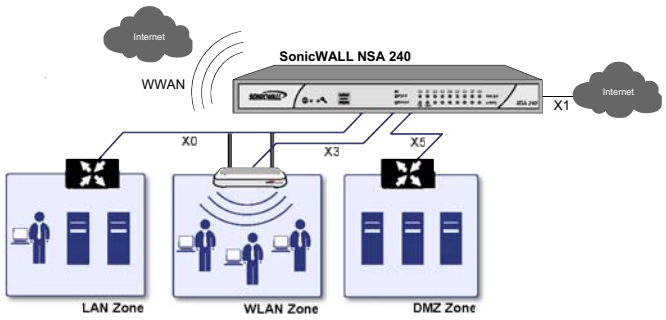
Troubleshooting Initial Setup

If you cannot connect to the SonicWALL NSA appliance or the **Setup Wizard** does not display, verify the following configurations:

- Did you correctly enter the management IP address in your Web browser?
- Are the Local Area Connection settings on your computer set to use DHCP or set to a static IP address on the 192.168.168.x/24 subnet?
- Do you have the Ethernet cable connected to your computer and to the **X0** (**LAN**) port on your SonicWALL?
- Is the connector clip on your network cable properly seated in the port of the security appliance?

Note: *Some pop-up blockers may prevent the launch of the Setup Wizard. You can temporarily disable your pop-up blocker, or add the management IP address of your SonicWALL (192.168.168.168 by default) to your pop-up blocker's allow list.*

Connecting to Your Network



The SonicWALL NSA 240 ships with the internal DHCP server active on the LAN port. However, if a DHCP server is already active on your LAN, the SonicWALL will disable its own DHCP server to prevent conflicts.

Ports X1 and X0 are preconfigured as WAN and LAN. The remaining ports (X2-X8) can be configured to meet the needs of your network. As an example, zones in the example above are configured as: X1: WAN, X2: LAN, X3: WLAN, and X5: DMZ.

Testing Your Connection

1. After you exit the Setup Wizard, the login page reappears. Log back into the management interface and verify your IP and WAN connection.
2. Ping a host on the Internet, such as sonicwall.com.
3. Open another Web browser and navigate to: <http://www.sonicwall.com>

   If you can view the SonicWALL home page, you have configured your SonicWALL NSA appliance correctly.

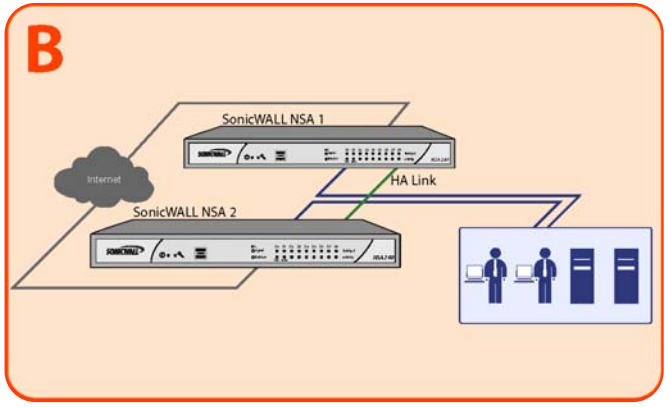
   If you cannot view the SonicWALL home page, renew your management station DHCP address.
4. If you still cannot view a Web page, try one of these solutions:
   - **Restart your Management Station** to accept new network settings from the DHCP server in the SonicWALL security appliance.
   - **Restart your Internet Router** to communicate with the DHCP Client in the SonicWALL security appliance.

Next... *Continue to Verifying Your Connection section, on page 35 to verify your WWAN connection.*

Scenario B: HA Pair in NAT/Route Mode

For network installations with two SonicWALL NSA 240 appliances configured as a stateful synchronized pair for redundant high availability networking.

In this scenario, one SonicWALL NSA 240 operates as the primary gateway device and the other SonicWALL NSA 240 is in passive mode. All network connection information is synchronized between the two devices so that the backup appliance can seamlessly switch to active mode without dropping any connections if the primary device loses connectivity.



This section provides instructions for configuring a pair of SonicWALL NSA appliances for High Availability (HA). This section is relevant to administrators following deployment **Scenario B**.

Note: *High Availability is supported for two SonicWALL NSA appliances of the same model.*

This section contains the following subsections:

- *Initial HA Setup* - page 25
- *Configuring HA* - page 26
- *Configuring Advanced High Availability Settings* - page 26
- *Synchronizing Settings* - page 28
- *Configuring HA License Overview* - page 29
- *Associating Pre-Registered Appliances* - page 30

Initial HA Setup

Before you begin the configuration of HA on the Primary SonicWALL security appliance, perform the following setup:

1. On the back panel of the Backup SonicWALL security appliance, locate the serial number and write the number down. You need to enter this number in the **High Availability** > **Settings** page.
2. Verify that the Primary SonicWALL and Backup SonicWALL security appliances are registered, running the same SonicOS Enhanced versions, and running the same SonicWALL Security services.
3. Make sure the Primary SonicWALL and Backup SonicWALL security appliances' LAN, WAN and other interfaces are properly configured for failover.
4. Connect the X8 ports on the Primary SonicWALL and Backup SonicWALL appliances with a CAT 5 Ethernet cable. The Primary and Backup SonicWALL security appliances must have a dedicated connection.
5. Power up the Primary SonicWALL security appliance, and then power up the Backup SonicWALL security appliance.
6. Do not make any configuration changes to the Primary's X8; the High Availability configuration in an upcoming step takes care of this issue.

Configuring HA

The first task in setting up HA after initial setup is configuring the **High Availability** > **Settings** page on the Primary SonicWALL security appliance. Once you configure HA on the Primary SonicWALL security appliance, it communicates the settings to the Backup SonicWALL security appliance.

To configure HA on the Primary SonicWALL, perform the following steps:

1. Navigate to the **High Availability** > **Settings** page.
2. Select the **Enable High Availability** checkbox.
3. Under **SonicWALL Address Settings**, type in the serial number for the Backup SonicWALL appliance.
   You can find the serial number on the back of the SonicWALL security appliance, or in the **System** > **Status** screen of the backup unit. The serial number for the Primary SonicWALL is automatically populated.
4. Click **Apply** to retain these settings.

Configuring Advanced High Availability Settings

1. Navigate to the **High Availability** > **Advanced** page.
2. To configure Stateful HA, select **Enable Stateful Synchronization**. A dialog box is displayed with recommended settings for the **Heartbeat Interval** and **Probe Interval** fields. The settings it shows are minimum recommended values. Lower values may cause unnecessary failovers, especially when the SonicWALL is under a heavy load. You can use higher values if your SonicWALL handles a lot of network traffic. Click **OK**.

Tip: *Preempt mode is recommended to be disabled after enabling Stateful Synchronization. This is because preempt mode can be over-aggressive about failing over to the backup appliance.*

3. To backup the firmware and settings when you upgrade the firmware version, select **Generate/Overwrite Backup Firmware and Settings When Upgrading Firmware**.
4. Select the **Enable Virtual MAC** checkbox. Virtual MAC allows the Primary and Backup appliances to share a single MAC address. This greatly simplifies the process of updating network ARP tables and caches when a failover occurs. Only the WAN switch to which the two appliances are connected to needs to be notified. All outside devices will continue to route to the single shared MAC address.

5. The **Heartbeat Interval** controls how often the two units communicate. The default is 5000 milliseconds; the minimum recommended value is 1000 milliseconds. Less than this may cause unnecessary failovers, especially when the SonicWALL is under a heavy load.
6. Typically, SonicWALL recommends leaving the **Heartbeat Interval**, **Election Delay Time (seconds)**, and **Dynamic Route Hold-Down Time** fields to their default settings. These fields can be tuned later as necessary for your specific network environment:
   - The **Failover Trigger Level** sets the number of heartbeats that can be missed before failing over. By default, this is set to 5 missed heartbeats.
   - The **Election Delay Time** is the number of seconds allowed for internal processing between the two units in the HA pair before one of them takes the primary role.
   - The **Probe Level** sets the interval in seconds between communication with upstream or downstream systems. The default is 20 seconds, and the allowed range is 5 to 255 seconds. You can set the Probe IP Address(es) on the **High Availability** > **Monitoring** screen.
   - The **Dynamic Route Hold-Down Time** setting is used when a failover occurs on a HA pair that is using either RIP or OSPF dynamic routing, and it is only displayed when the **Advanced Routing** option is selected on the **Network** > **Routing** page. When a failover occurs, **Dynamic Route Hold-Down Time** is the number of seconds the newly-active appliance keeps the dynamic routes it had previously learned in its route table. During this time, the newly-active appliance relearns the dynamic routes in the network. When the **Dynamic Route Hold-Down Time** duration expires, it deletes the old routes and implements the new routes it has learned from RIP or OSPF. The default value is 45 seconds. In large or complex networks, a larger value may improve network stability during a failover.
7. Select the **Include Certificates/Keys** checkbox to have the appliances synchronize all certificates and keys.
8. Click **Synchronize Settings** to synchronize the settings between the Primary and Backup appliances.
9. Click **Synchronize Firmware** if you previously uploaded new firmware to your Primary unit while the Secondary unit was offline, and it is now online and ready to upgrade to the new firmware. **Synchronize Firmware** is typically used after taking your Secondary appliance offline while you test a new firmware version on the Primary unit before upgrading both units to it.
10. Click **Apply** to retain the settings on this screen.

Synchronizing Settings

Once you have configured the HA settings on the Primary SonicWALL security appliance, it will automatically synchronize the settings to the Backup unit, causing the Backup to reboot. You do not need to click the **Synchronize Settings** button. However, if you later choose to do a manual synchronization of settings, click the **Synchronize Settings** button. You will see a **HA Peer Firewall has been updated** notification at the bottom of the management interface page. Also note that the management interface displays **Logged Into: Primary SonicWALL Status: (green ball) Active** in the upper-right-hand corner.

By default, the **Include Certificate/Keys** setting is enabled. This specifies that certificates, certificate revocation lists (CRL), and associated settings are synchronized between the Primary and Backup units. When local certificates are copied to the Backup unit, the associated private keys are also copied. Because the connection between the Primary and Backup units is typically protected, this is generally not a security concern.

Tip: *A compromise between the convenience of synchronizing certificates and the added security of not synchronizing certificates is to temporarily enable the **Include Certificate/Keys** setting and manually synchronize the settings, and then disable **Include Certificate/Keys**.*

To verify that Primary and Backup SonicWALL security appliances are functioning correctly, wait a few minutes, then trigger a test failover by logging into the Primary unit and doing a restart. The Backup SonicWALL security appliance should quickly take over.

From your management workstation, test connectivity through the Backup SonicWALL by accessing a site on the public Internet – note that the Backup SonicWALL, when active, assumes the complete identity of the Primary, including its IP addresses and Ethernet MAC addresses.

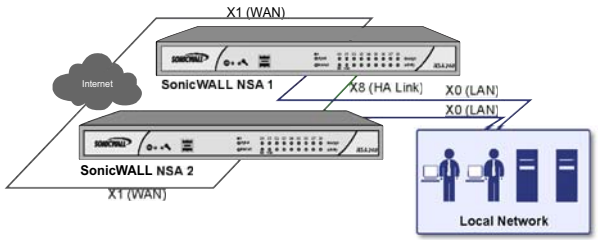
Log into the Backup SonicWALL's unique LAN IP address. The management interface should now display **Logged Into: Backup SonicWALL Status: (green ball) Active** in the upper-right-hand corner.

Now, power the Primary SonicWALL back on, wait a few minutes, then log back into the management interface. If stateful synchronization is enabled (automatically disabling preempt mode), the management GUI should still display **Logged Into: Backup SonicWALL Status: (green ball) Active** in the upper-right-hand corner.

If you are using the Monitor Interfaces feature, experiment with disconnecting each monitored link to ensure correct configuration.

Configuring HA License Overview

You can configure HA license synchronization by associating two SonicWALL security appliances as HA Primary and HA Secondary on MySonicWALL. Note that the Backup appliance of your HA pair is referred to as the HA Secondary unit on MySonicWALL.



You must purchase a single set of security services licenses for the HA Primary appliance. To use Stateful HA, you must first activate the Stateful High Availability Upgrade license for the primary unit in SonicOS. This is automatic if your appliance is connected to the Internet. See *Registering and Licensing Your Appliance on MySonicWALL - page 13*.

GATEWAY SERVICES

Service Name	Info	Status	
Gateway AV/Anti-Spyware/Intrusion Prevention/Application Firewall		Expiry: 24 Mar 2008	Buy
Content Filtering: Premium Edition		-	Buy
VPN Upgrade		veal-fee-marc-wake-volt-gad	

License synchronization is used during HA so that the Backup appliance can maintain the same level of network protection provided before the failover. To enable HA, you can use the SonicOS UI to configure your two appliances as a HA pair in Active/Idle mode.

MySonicWALL provides several methods of associating the two appliances. You can start by registering a new appliance, and then choosing an already-registered unit to associate it with. You can associate two units that are both already registered. Or you can select a registered unit and then add a new appliance with which to associate it.

Note: *After registering new SonicWALL appliances on MySonicWALL, you must also register each appliance from the SonicOS management interface by clicking the registration link on the **System** > **Status** page. This allows each unit to synchronize with the SonicWALL license server and share licenses with the associated appliance.*

Associating Pre-Registered Appliances

To associate two already-registered SonicWALL security appliances so that they can use HA license synchronization, perform the following steps:

1. Login to MySonicWALL and click **My Products**.
2. On the My Products page, under Registered Products, scroll down to find the appliance that you want to use as the parent, or primary, unit. Click the product **name** or **serial number**.
3. On the Service Management - Associated Products page, scroll down to the Associated Products section.
4. Under Associated Products, click **HA Secondary**.
5. On the My Product - Associated Products page, in the text boxes under Associate New Products, type the **serial number** and the friendly **name** of the appliance that you want to associate as the child/secondary/backup unit.
6. Select the group from the **Product Group** drop-down list. The product group setting specifies the MySonicWALL users who can upgrade or modify the appliance.
7. Click **Register**.
8. Continue to *Additional Deployment Configuration - page 47*.

Note: *For additional reference, refer to the* SonicOS Enhanced High Availability License Sync *product guide at:* <http://www.sonicwall.com/us/Support.html>

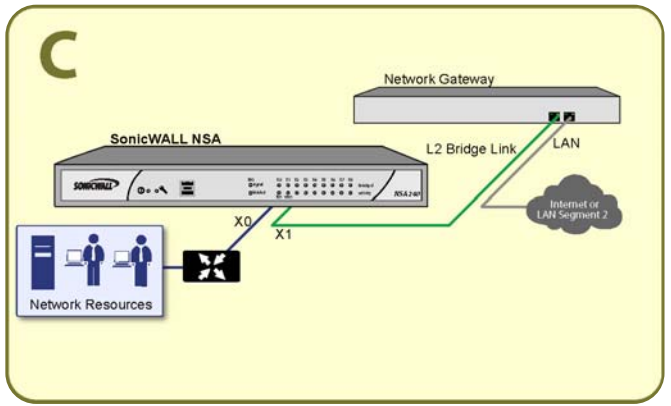
Next... *Continue to the Verifying Your Connection section, on page 35 to verify your WWAN connection.*

Scenario C: L2 Bridge Mode

For network installations where the SonicWALL NSA 240 is running in tandem with an existing network gateway.

In this scenario, the original gateway is maintained. The SonicWALL NSA 240 is integrated seamlessly into the existing network, providing the benefits of deep packet inspection and comprehensive security services on all network traffic.

L2 Bridge Mode employs a secure learning bridge architecture, enabling it to pass and inspect traffic types that cannot be handled by many other methods of transparent security appliance integration. Using L2 Bridge Mode, a SonicWALL security appliance can be non-disruptively added to any Ethernet network to provide in-line deep packet inspection for all traversing IPv4 TCP and UDP traffic. L2 Bridge Mode can pass all traffic types, including IEEE 802.1Q VLANs, Spanning Tree Protocol, multicast, broadcast, and IPv6.



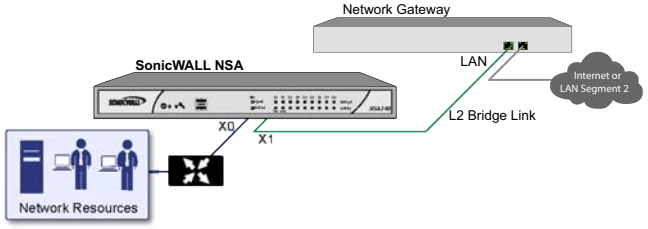
This section provides instructions to configure the SonicWALL NSA appliance in tandem with an existing Internet gateway device. This section is relevant to users following deployment **Scenario C**.

This section contains the following subsections:

- *Connection Overview - page 32*
- *Configuring the Primary Bridge Interface* - page 32
- *Configuring the Secondary Bridge Interface* - page 33

Connection Overview

Connect the X1 port on your SonicWALL NSA 240 to the LAN port on your existing Internet gateway device. Then connect the X0 port on your SonicWALL to your LAN.



Configuring the Primary Bridge Interface

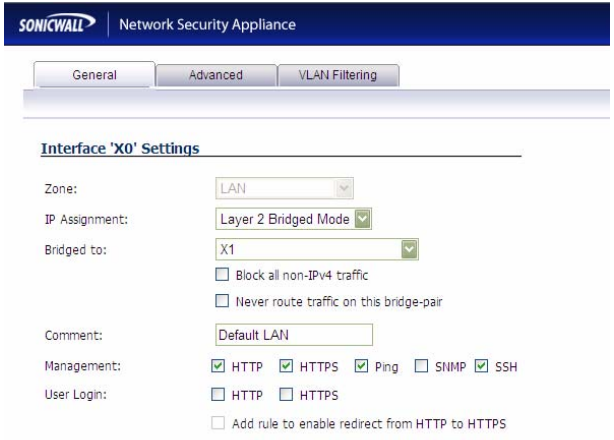
The primary bridge interface is your existing Internet gateway device. The only step involved in setting up your primary bridge interface is to ensure that the WAN interface is configured for a static IP address. You will need this static IP address when configuring the secondary bridge.

Note: *The primary bridge interface must have a static IP assignment.*

Configuring the Secondary Bridge Interface

Complete the following steps to configure the SonicWALL appliance:

1. Navigate to **Network** > **Interfaces**.
2. Click the Configure icon in the right column of the X0 (LAN) interface.



3. In the **IP Assignment** drop-down list, select **Layer 2 Bridge Mode**.
4. In the **Bridged to** drop-down list, select the **X1** interface.
5. Configure management options (HTTP, HTTPS, Ping, SNMP, SSH, User logins, or HTTP redirects).
6. Click **OK**.

Note: *Do not enable **Never route traffic on the bridge-pair** unless your network topology requires that all packets entering the L2 Bridge remain on the L2 Bridge segments.*

*You may optionally enable the **Block all non-IPv4 traffic** setting to prevent the L2 bridge from passing non-IPv4 traffic.*

Next... *Continue to Verifying Your Connection section, on page 35 to verify your WWAN connection.*

Verifying Your Connection 5

In this Section:

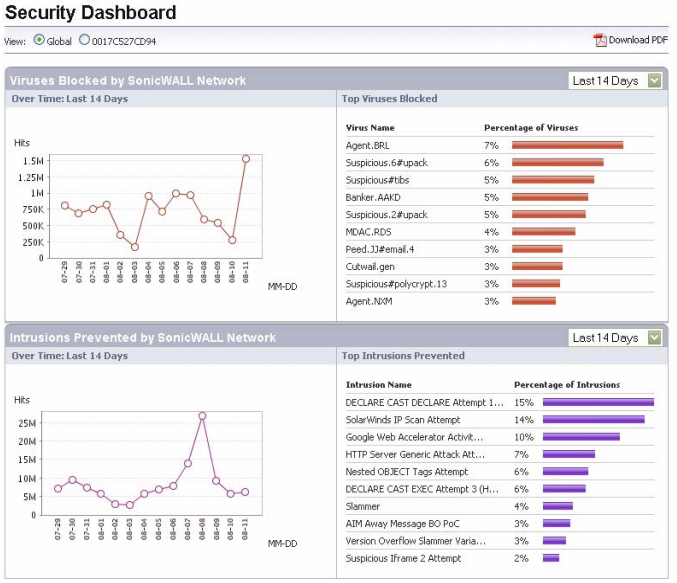
This section provides instructions to ensure proper connectivity of your SonicWALL NSA 240 appliance.

- *Verifying Management Interface Connectivity* - page 36
- *Verifying WAN (Internet) Connectivity* - page 37
- *Viewing the WWAN Connection Status* - page 37
- *Managing the WWAN Connection Status* - page 38
- *Verifying WWAN Failover Functionality* - page 38

Verifying Management Interface Connectivity

1. If your SonicWALL did not require a restart, skip to the *Verifying WAN (Internet) Connectivity* section, on page 37. Otherwise, continue with step 2.
2. Wait for the SonicWALL NSA 240 to reboot. When the Test LED is no longer lit, the SonicWALL NSA 240 is ready for login.
3. If the login page does not display after reboot, open a Web browser on the computer and manually navigate to the LAN IP address of your SonicWALL NSA 240.
4. Using your new **username** and **password**, login to the appliance.

If the **System > Security Dashboard** page (shown below) displays, then you have correctly configured the SonicWALL NSA 240 to work with the computer on your LAN. Complete the next section to verify WAN (Internet) connectivity.



Verifying WAN (Internet) Connectivity

Complete the following steps to confirm your Internet connectivity.

1. In the Windows interface of a computer connected to the LAN port, select **Start > Run**.
2. Enter “cmd” in the **Open** field and click the **OK** button.
3. At the prompt, type the command “ping www.sonicwall.com” and press **Enter** on the keyboard.

C:\Documents and Settings\hha>ping www.sonicwall.com
Pinging www.global.sonicwall.com [204.212.170.111] with 32 bytes of data:
Reply from 204.212.170.111: bytes=32 time=8ms TTL=58
Reply from 204.212.170.111: bytes=32 time=15ms TTL=58
Reply from 204.212.170.111: bytes=32 time=27ms TTL=58
Reply from 204.212.170.111: bytes=32 time=7ms TTL=58
Ping statistics for 204.212.170.111:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 7ms, Maximum = 27ms, Average = 14ms

If the ping times out, you may have to renew your computer’s IP address.

4. If the ping is successful, use your Web browser to navigate to a Website, such as: <http://www.sonicwall.com/>
   If the Website displays, your SonicWALL NSA 240 is configured correctly as your gateway device.

Viewing the WWAN Connection Status

The **Network > Interfaces** page allows you to view the current WWAN connection status.

1. Log into the SonicWALL NSA 240 appliance management interface.
2. Navigate to **Network > Interfaces**.
3. In the Interface Settings section, the WWAN interface line displays the current status as follows:

The following messages describe the status of the WWAN interface:

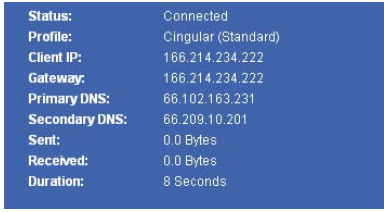
On hook	Indicates that the WWAN card is present but not yet connected.
Connected and starting PPP authentication	Indicates that the WWAN card is associated and currently attempting a connection to the WWAN network.
Connected	Indicates an active connection.

Managing the WWAN Connection Status

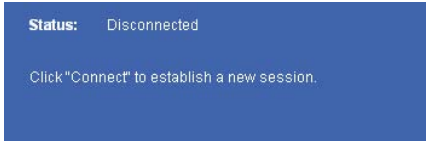
The Connection Manager window allows you to connect, disconnect, and view current WWAN connection status.

1. In the SonicWALL NSA 240 appliance management interface, navigate to **Network > Interfaces**.
2. In the Interface Settings section, under WWAN, click the **Manage** button.

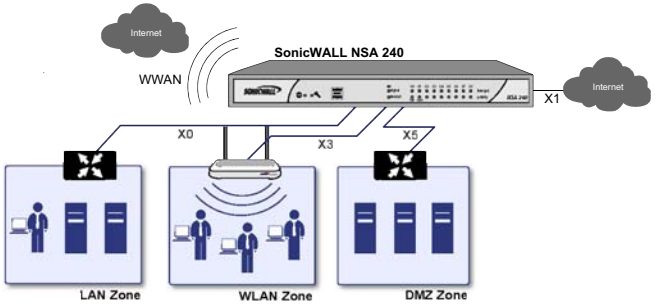
3. The Connection Manager windows displays your connection status.



4. If the Connection Manager shows “disconnected,” click the **Connect** button. You will connect to a network if one is available.



Verifying WWAN Failover Functionality



Complete the following steps to confirm your WWAN Internet connectivity.

1. Unplug your appliance’s WAN port (if you plugged it in during the initial setup).
2. Wait a few moments for the NSA 240 to failover to the WWAN for Internet connectivity. Refer to the front panel of the appliance to see when the WWAN PC card shows activity.
3. Launch a Website, such as <*http://www.sonicwall.com*> in a browser, using a computer that is connected to the SonicWALL NSA 240 appliance and using the SonicWALL as its sole Internet connection.

If the Website displays, your SonicWALL NSA 240 is operational and connected to a valid WWAN service provider account. Remember to plug the WAN back in if you wish to use WWAN as a failover.

Enabling Essential Security Services 6

In this Section:

Security services are an essential component of a secure network deployment. This section provides instructions for registering and enabling security services on your SonicWALL NSA 240 appliance.

- *Activating Licenses in SonicOS* - page 40
- *Enabling Security Services in SonicOS* - page 40
- *Applying Security Services to Network Zones* - page 46

Activating Licenses in SonicOS

After completing the registration process in SonicOS, you must perform the following tasks to activate your licenses and enable your licensed services from within the SonicOS user interface:

- Activate licenses
- Enable security services
- Apply services to network zones

To activate licensed services in SonicOS, you can enter the license keyset manually, or you can synchronize all licenses at once with MySonicWALL.

The Setup Wizard automatically synchronizes all licenses with MySonicWALL if the appliance has Internet access during initial setup. If initial setup is already complete, you can synchronize licenses from the **System** > **Licenses** page.

Manual upgrade using the license keyset is useful when your appliance is not connected to the Internet. The license keyset includes all license keys for services or software enabled on MySonicWALL. It is available on <http://www.sonicwall.com> at the top of the Service Management page for your SonicWALL NSA appliance.

To activate licenses in SonicOS:

1. Navigate to the **System** > **Licenses** page.
2. Under Manage Security Services Online do one of the following:
   - Enter your MySonicWALL credentials, then click the **Synchronize** button to synchronize licenses with MySonicWALL.
   - Paste the license keyset into the **Manual Upgrade Keyset** field.
3. Click **Submit**.

Enabling Security Services in SonicOS

SonicWALL security services are key components of threat management in SonicOS. The core security services are Gateway Anti-Virus, Intrusion Prevention Services, and Anti-Spyware.

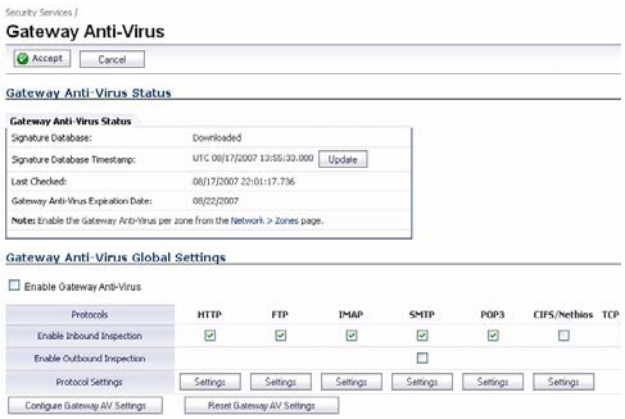
You must enable each security service individually in the SonicOS user interface. See the following procedures to enable and configure the three security services that must be enabled:

- *Enabling Gateway Anti-Virus - page 41*
- *Enabling Intrusion Prevention Services - page 42*
- *Enabling Anti-Spyware - page 43*
- *Enabling Content Filtering Service - page 44*

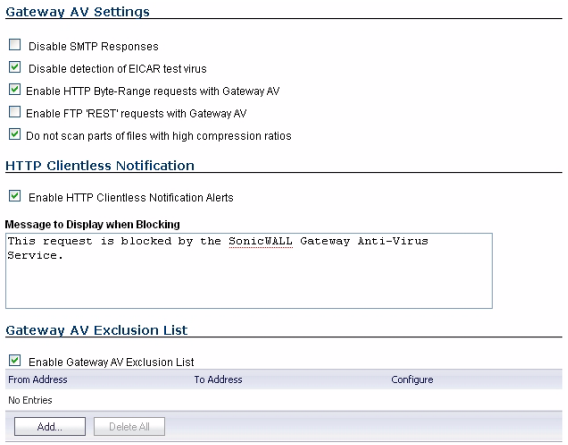
Enabling Gateway Anti-Virus

To enable Gateway Anti-Virus in SonicOS:

1. Navigate to the **Security Services** > **Gateway Anti-Virus** page. Select the **Enable Gateway Anti-Virus** checkbox.



2. Select the **Enable Inbound Inspection** checkboxes for the protocols to inspect. By default, SonicWALL GAV inspects all inbound **HTTP**, **FTP**, **IMAP**, **SMTP** and **POP3** traffic. **CIFS/NetBIOS** can optionally be enabled to allow access to shared files. Generic **TCP Stream** can optionally be enabled to inspect all other TCP based traffic, such as non-standard ports of operation for SMTP and POP3, and IM and P2P protocols.
3. Enabling **Outbound Inspection** for SMTP scans mail for viruses before it is delivered to an internally hosted SMTP server.
4. For each protocol you can restrict the transfer of files with specific attributes by clicking on the **Settings** button under the protocol. In the Settings dialog box, you can configure the following:
   - **Restrict Transfer of password-protected Zip files** - Disables the transfer of password protected ZIP files over any enabled protocol. This option only functions on protocols that are enabled for inspection.
   - **Restrict Transfer of MS-Office type files containing macros (VBA 5 and above)** - Disables the transfers of any MS Office files that contain VBA macros.
   - **Restrict Transfer of packed executable files (UPX, FSG, etc.)** - Disables the transfer of packed executable files. Packers are utilities that compress and encrypt executables. Although there are legitimate applications for these, they can be used with the intent of obfuscation, and can make the executables less detectable by anti-virus applications. The packer adds a header that expands the file in memory, and then executes that file. SonicWALL Gateway Anti-Virus currently recognizes the most common packed formats: UPX, FSG, PKLite32, Petite, and ASPack,
5. Click **Configure Gateway AV Settings**. The **Gateway AV Settings** window allows you to configure clientless notification alerts and create a SonicWALL GAV exclusion list.

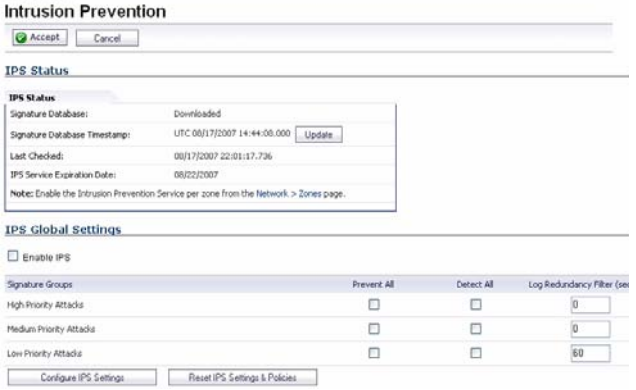

Gateway AV Settings
Disable SMTP Responses
Disable detection of EICAR test virus
Enable HTTP Byte-Range requests with Gateway AV
Enable FTP 'REST' requests with Gateway AV
Do not scan parts of files with high compression ratios
HTTP Clientless Notification
Enable HTTP Clientless Notification Alerts
Message to Display when Blocking
This request is blocked by the SonicWALL Gateway Anti-Virus Service.
Gateway AV Exclusion List
Enable Gateway AV Exclusion List
From Address
To Address
Configure
No Entries
Add...
Delete All

6. Select the **Disable SMTP Responses** box to suppress the sending of email messages to clients from SonicWALL GAV when a virus is detected in an email or attachment.
7. Select **Enable HTTP Clientless Notification Alerts** and customize the message to be displayed when GAV detects a threat from the HTTP server.
8. Select **Enable Gateway AV Exclusion List** and then click **Add** to define a range of IP addresses whose traffic will be excluded from SonicWALL GAV scanning.
9. When finished in the Add GAV Range dialog box, click **OK**.
10. In the Gateway AV Config View window, click **OK**.
11. In the **Security Services** > **Gateway Anti-Virus** page, click **Accept**.

Enabling Intrusion Prevention Services

To enable Intrusion Prevention Services in SonicOS:

1. Navigate to the **Security Services** > **Intrusion Prevention** page. Select the **Enable Intrusion Prevention** checkbox.



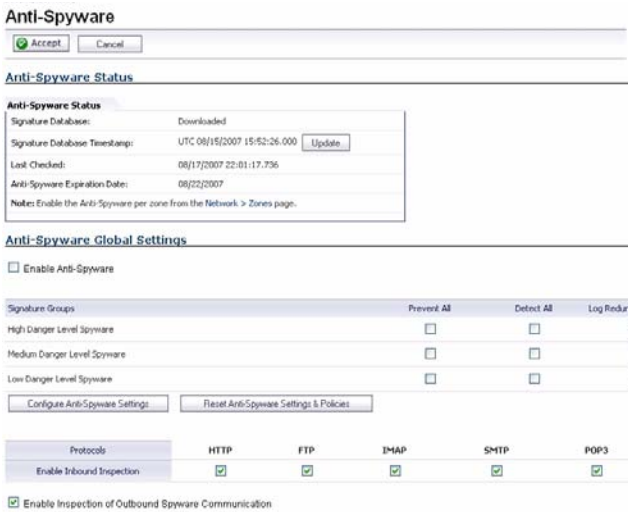
2. In the Signature Groups table, select the **Prevent All** and **Detect All** checkboxes for each attack priority that you want to prevent. Selecting the **Prevent All** and **Detect All** check boxes for **High Priority Attacks** and **Medium Priority Attacks** protects your network against the most dangerous and disruptive attacks.

3. To log all detected attacks, leave the **Log Redundancy Filter** field set to zero. To enforce a delay between log entries for detections of the same attack, enter the number of seconds to delay.
4. Click **Configure IPS Settings** to enable IP packet reassembly before inspection and create a SonicWALL IPS exclusion list.
5. In the IPS Config View window, select **Enable IPS Exclusion List** and then click **Add** to define a range of IP addresses whose traffic will be excluded from SonicWALL IPS scanning.
6. When finished in the Add IPS Range dialog box, click **OK**.
7. In the IPS Config View window, click **OK**.
8. In the **Security Services** > **Intrusion Prevention** page, click **Accept**.

Enabling Anti-Spyware

To enable Anti-Spyware in SonicOS:

1. Navigate to the **Security Services** > **Anti-Spyware** page. Select the **Enable Anti-Spyware** checkbox.

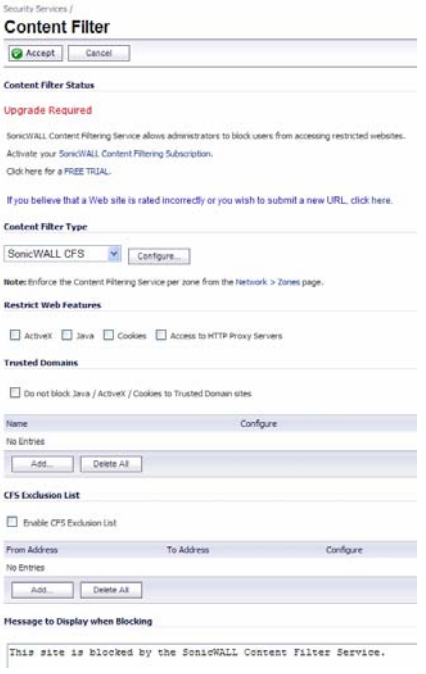


2. In the Signature Groups table, select the **Prevent All** and **Detect All** checkboxes for each spyware danger level that you want to prevent.

3. To log all spyware attacks, leave the **Log Redundancy Filter** field set to zero. To enforce a delay between log entries for detections of the same attack, enter the number of seconds to delay.
4. Click **Configure Anti-Spyware Settings** to configure clientless notification alerts and create a SonicWALL Anti-Spyware exclusion list.
5. Select the **Disable SMTP Responses** box to suppress the sending of email messages to clients from SonicWALL Anti-Spyware when spyware is detected in an email or attachment.
6. Select **Enable HTTP Clientless Notification Alerts** and customize the message to be displayed in the browser when SonicWALL Anti-Spyware detects a threat from the HTTP server.
7. Select **Enable Anti-Spyware Exclusion List** and then click **Add** to define a range of IP addresses whose traffic will be excluded from SonicWALL Anti-Spyware scanning.
8. When finished in the Add Anti-Spyware Range dialog box, click **OK**.
9. In the Anti-Spyware Config View window, click **OK**.
10. Select the **Enable Inbound Inspection** checkboxes for the protocols to inspect. By default, SonicWALL GAV inspects all inbound **HTTP**, **FTP**, **IMAP**, **SMTP**, and **POP3** traffic.
11. Select the **Enable Inspection of Outbound Communication** checkbox to enable scanning of traffic that originates internally.
12. On the **Security Services** > **Anti-Spyware** page, click **Accept**.

Enabling Content Filtering Service

The default Content Filtering Service (CFS) policy is available with or without a CFS subscription. The **Security Services > Content Filter** page provides links to purchase a license or get a free trial, and displays subscription status and basic configuration settings.



You can enforce or disable content filtering on each zone from the **Network > Zones** page, as described in the *Applying Security Services to Network Zones* section, on page 46.

With a valid CFS subscription, you can create custom CFS policies and apply them to network zones or to groups of users. For example, a school could create one policy for teachers and another for students.

For complete information about activating and configuring SonicWALL CFS, see the *SonicWALL Content Filtering Service Premium Administrator's Guide* or *SonicWALL Content Filtering Service Standard Administrator's Guide*.

Content Filtering Service (CFS) Bypass for Administrators

The **Do not bypass CFS blocking for the administrator** checkbox controls content filtering for administrators. By default, when the administrator ("admin" user) is logged into the SonicOS management interface from a system, CFS blocking is suspended for that system's IP address for the duration of the authenticated session. If you prefer to provide content filtering and apply CFS policies to the IP address of the administrator's system, perform the following steps:

1. Select the **Do not bypass CFS blocking for the Administrator checkbox**.
2. Click **Accept**.

Enabling and Adding to the CFS Exclusion List

To enable the CFS Exclusion List and add a range of IP addresses to it, perform the following steps:

1. Select the **Enable CFS Exclusion List** checkbox.
2. Click **Add**. The **Add CFS Range Entry** window is displayed.
3. Enter the first IP address in the excluded range into the **IP Address From:** field and the last address into the **IP Address To:** field.
4. Click **OK**. The IP address range is added to the CFS Exclusion List.
5. On the **Security Services > Content Filter** page, click **Accept**.

Disabling, Editing, or Deleting Addresses from the CFS Exclusion List

You can temporarily disable CFS exclusions without removing all entries from the list. You can also delete some or all IP address ranges from the CFS Exclusion List.

1. To keep the CFS Exclusion List entries, but temporarily allow content filtering policies to be applied to these IP addresses, uncheck the **Enable CFS Exclusion List** checkbox. This disables CFS exclusions.
2. To edit a trusted domain entry, click the pencil icon in the Configure column.
3. To delete an individual trusted domain from the CFS Exclusion List, click the **Delete** icon for the entry in the Configure column.

4. To delete all trusted domains from the CFS Exclusion List, click **Delete All**.
5. On the **Security Services > Content Filter** page, click **Accept**.

Applying Security Services to Network Zones

A network zone is a logical group of one or more interfaces to which you can apply security rules to regulate traffic passing from one zone to another zone.

Security services such as Gateway Anti-Virus are automatically applied to the LAN and WAN network zones. To protect other zones such as the DMZ or Wireless LAN (WLAN), you must apply the security services to the network zones. For example, you can configure SonicWALL Intrusion Prevention Service for incoming and outgoing traffic on the WLAN zone to add more security for internal network traffic.

To apply services to network zones:

1. Navigate to the **Network** > **Zones** page.
2. In the Zone Settings table, click the **Configure** icon for the zone where you want to apply security services.
3. In the Edit Zone dialog box on the General tab, select the checkboxes for the security services to enable on this zone.
4. On the Edit Zone page, select the checkboxes for the security services that you want to enable.
5. Click **OK**.
6. To enable security services on other zones, repeat steps 2 through step 4 for each zone.

Additional Deployment Configuration 7

In this Section:

This section provides basic configuration information to begin building network security policies for your deployment. This section also contains several SonicOS diagnostic tools and a deployment configuration reference checklist.

- *Manually Configuring WWAN Failover* - page 48
- *Configuring Additional Interfaces* - page 48
- *Configuring PortShield Interfaces* - page 52
- *Creating Network Access Rules* - page 52
- *Creating a NAT Policy* - page 55
- *Upgrading Firmware on Your SonicWALL* - page 58
- *Deploying SonicPoints for Wireless Access* - page 61
- *Troubleshooting Diagnostic Tools* - page 66
- *Deployment Configuration Reference Checklist* - page 70

Manually Configuring WWAN Failover

To manually configure WWAN Failover:

1. Navigate to the **WWAN** > **Connection Profiles** page. Under **Connection Profiles**, click **Add**.
2. On the **General** tab, specify **Country**, **Service Provider**, and **Plan Type**. Click **OK**.

Note: *If you are unsure about your Plan Type, select Standard.*

3. Next, navigate to the **Network** > **Interfaces** page.
4. Verify the **WAN Connection Model** is set to **Ethernet with WWAN Failover**.

Note: *If you WWAN service plan is bandwidth/time limited, enable **Configure Data Usage Limiting** to stay within your plan's limitations.*

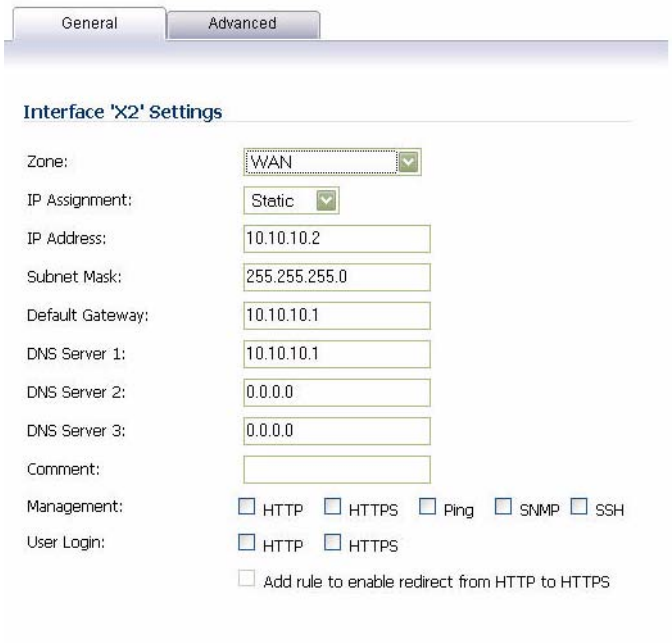
Configuring Additional Interfaces

The SonicOS Enhanced Web-based management interface allows you to configure two ports as WAN interfaces. Port X1 is preconfigured as the WAN. You have the option of choosing another port (X2-X8) to configure as a second WAN interface.

To configure a second WAN interface:

1. Click the Configure icon of the port you wish to configure as the second WAN interface.
2. In the **Zone** list, select **WAN**. Specify the settings for this interface. Click **OK** when you are finished.

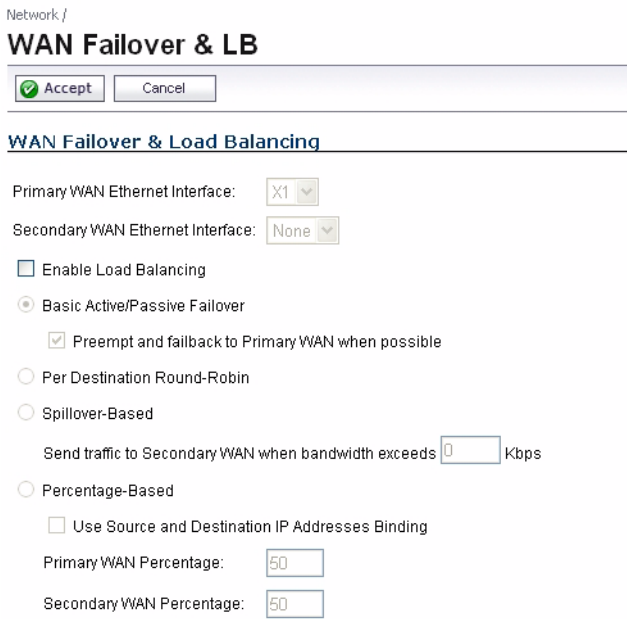
Note: *For more information regarding WAN Interfaces, see the SonicOS Enhanced Administrator's Guide - Configuring Interfaces section.*



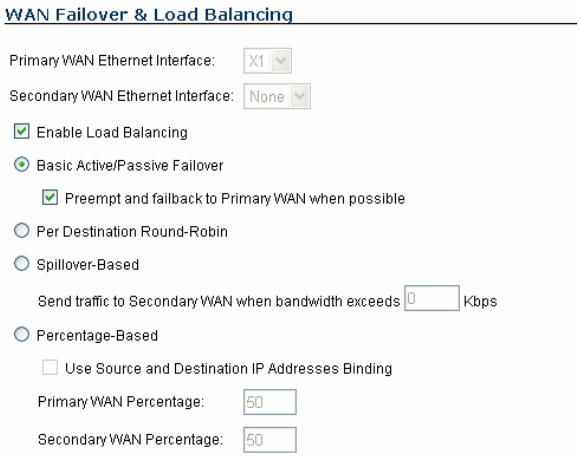
Activating WAN Failover and Selecting the Load Balancing Method

To configure the SonicWALL for WAN failover and load balancing, follow the steps below:

1. On the **Network > WAN Failover & LB** page, select Enable Load Balancing.



2. If there are multiple possible secondary WAN interfaces, select an interface from the **Secondary WAN Ethernet Interface**.
3. Select a load balancing method. By default, the SonicWALL will select **Basic Active/Passive Failover** as a method, but there are four load balancing methods available:



Note: *For more information regarding WAN Failover and Load Balancing, see the SonicOS Enhanced Administrator's Guide.*

- **Basic Active/Passive Failover**—Sends traffic through the Secondary WAN interface if the Primary WAN interface has been marked inactive. This item has an associated **Preempt and fail back to Primary WAN when possible** checkbox. When selected, the SonicWALL security appliance switches back to sending its traffic across the Primary WAN interface when it resumes responding to the SonicWALL security appliance's checks.
- **Per Destination Round-Robin**—Load balances outgoing traffic on a per-destination basis. This is a simple load balancing method that allows you to utilize both links in a basic fashion.
- **Spillover-Based**—When this setting is selected, the user can specify when the SonicWALL security appliance starts sending traffic through the Secondary WAN interface. Specify the maximum allowed bandwidth on the primary WAN interface in the **Send traffic to Secondary WAN interface when bandwidth exceeds _ Kbps** field.
- **Percentage-Based**—When this setting is selected, you can specify the percentages of traffic sent through the Primary WAN and Secondary WAN interfaces, utilizing both interfaces.
  - **Use Source and Destination IP Address Binding**—This checkbox enables you to maintain a consistent mapping of traffic flows with a single outbound WAN interface, regardless of the percentage of traffic through that interface.

4. Click **Accept**.

WAN Probe Monitoring

Enabling probe monitoring on the Network > WAN Failover & Load Balancing page instructs the SonicWALL security appliance to perform logical checks of upstream targets to ensure that the line is indeed usable, eliminating this potential problem, as well as continue to do physical monitoring. Under the default probe monitoring configuration, the SonicWALL performs an ICMP ping probe of both WAN ports' default gateways. Unfortunately, this is also not an assured means of link monitoring because service interruption may be occurring further upstream.

To perform reliable link monitoring, you can choose ICMP or TCP as monitoring method, and can specify up to two targets for each WAN port. TCP is preferred because many devices on the public Internet now actively drop or block ICMP requests. If you specify two targets for each WAN interface, you can logically link the two probe targets such that if either one fails the line will go down, or that both must fail for the line to be considered down. Using the latter method, you can configure a sort of 'deep check' to see if the line is truly usable – for instance, you could set first probe target of your ISP's router interface using ICMP (assuming they allow this), and then do a secondary probe target of a DNS server on the public Internet using TCP Port 53. With this method, if the ICMP probe of the ISP's router fails but the farther upstream continues to respond, the SonicWALL security appliance assumes the link is usable and continues to send traffic across it.

Note: *For more information regarding WAN Probe Monitoring, see the SonicOS Enhanced Administrator's Guide.*

Configuring PortShield Interfaces

The SonicWALL PortShield feature enables you to configure some or all of the switch ports on the SonicWALL NSA 240 appliance into separate contexts, or PortShield interfaces, providing protection from traffic on the LAN, WAN, and DMZ, as well as the devices inside your network. Each context has its own wire-speed switch ports that have protection of a dedicated, deep-packet inspection firewall.

To Configure Switch Ports Using SonicWALL PortShield:

1. On the **Network** > **Interfaces** page, click the **PortShield Wizard** button. This will run the SonicWALL PortShield Setup Wizard. Read the Introduction and click **Next**.
2. Select the appropriate groupings of SwitchPort interfaces for the SonicWALL NSA 240 appliance. Click **Next** to continue.This will prompt a configuration summary to appear. Verify the ports assigned are correct.
3. Click **Apply** to change port assignments.

Note: *If you select* WAN/DMZ/LAN Switch*, the X3-X8 ports will all be in a single PortShield group. Navigate to* ***Network*** > ***Interfaces*** *to enable or disable PortShield on each port.*

For more information about SwitchPort interfaces, see the *SonicOS Enhanced Administrator's Guide*.

Creating Network Access Rules

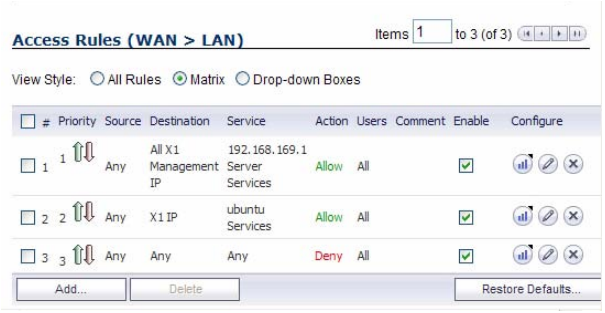
A Zone is a logical grouping of one or more interfaces designed to make management, such as the definition and application of access rules, a simpler and more intuitive process than following a strict physical interface scheme.

By default, the SonicWALL security appliance's stateful packet inspection allows all communication from the LAN to the Internet, and blocks all traffic from the Internet to the LAN. The following behaviors are defined by the "Default" stateful inspection packet access rule enabled in the SonicWALL security appliance:

Originating Zone	Destination Zone	Action
LAN, WLAN	WAN, DMZ	Allow
DMZ	WAN	Allow
WAN	DMZ	Deny
WAN and DMZ	LAN or WLAN	Deny

To create an access rule:

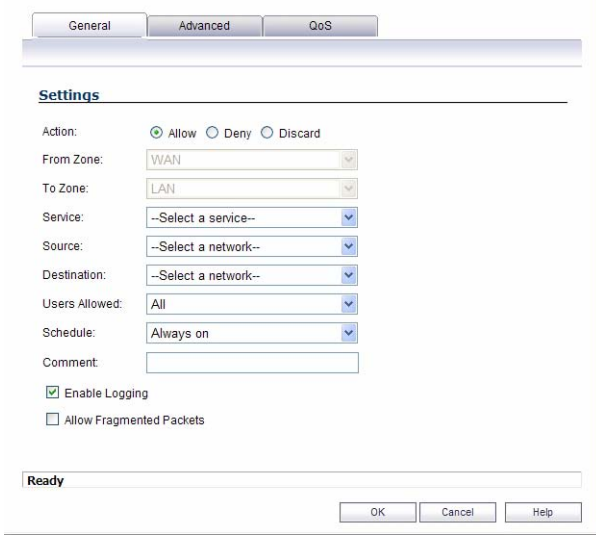
1. On the **Firewall** > **Access Rules** page in the matrix view, select two zones that will be bridged by this new rule.
   - On the Access Rules page, click **Add**.


Access Rules (WAN > LAN)
Items 1 to 3 (of 3)
View Style: All Rules Matrix Drop-down Boxes
Priority Source Destination Service Action Users Comment Enable Configure
1 1 Any All X1 Management IP 192.168.169.1 Server Services Allow All
2 2 Any X1 IP ubuntu Services Allow All
3 3 Any Any Any Deny All
Add... Delete Restore Defaults...

The access rules are sorted from the most specific at the top to the least specific at the bottom of the table. At the bottom of the table is the **Any** rule.

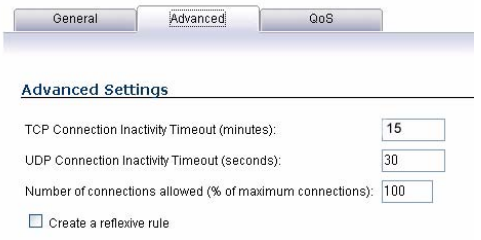
Note: *SonicWALL's default firewall rules are set in this way for ease of initial configuration, but do not reflect best practice installations. Firewall rules should only allow the required traffic and deny all other traffic.*

2. In the Add Rule page in the **General** tab, select **Allow** or **Deny** or **Discard** from the **Action** list to permit or block IP traffic.



- Select the service or group of services affected by the access rule from the **Service** drop-down list. If the service is not listed, you must define the service in the **Add Service** window. Select **Create New Service** or **Create New Group** to display the **Add Service** window or **Add Service Group** window.
- Select the source of the traffic affected by the access rule from the **Source** drop-down list. Selecting **Create New Network** displays the **Add Address Object** window.
- Select the destination of the traffic affected by the access rule from the **Destination** drop-down list. Selecting **Create New Network** displays the **Add Address Object** window.
- Select a user or user group from the **Users Allowed** drop-down list.
- Select a schedule from the **Schedule** drop-down list. The default schedule is **Always on**.
- Enter any comments to help identify the access rule in the **Comments** field.

3. Click on the **Advanced** tab.



   - In the **TCP Connection Inactivity Timeout (minutes)** field, set the length of TCP inactivity after which the access rule will time out. The default value is **15** minutes.
   - In the **UDP Connection Inactivity Timeout (minutes)** field, set the length of UDP inactivity after which the access rule will time out. The default value is **30** minutes.
   - In the **Number of connections allowed (% of maximum connections)** field, specify the percentage of maximum connections that is allowed by this access rule. The default is 100%.
   - Select **Create a reflexive rule** to create a matching access rule for the opposite direction, that is, from your destination back to your source.
4. Click on the **QoS** tab to apply DSCP or 802.1p Quality of Service coloring/marking to traffic governed by this rule.
5. Click **OK** to add the rule.

Creating a NAT Policy

The Network Address Translation (NAT) engine in SonicOS Enhanced allows users to define granular NAT policies for their incoming and outgoing traffic. By default, the SonicWALL security appliance has a preconfigured NAT policy to perform Many-to-One NAT between the systems on the LAN and the IP address of the WAN interface. The appliance does not perform NAT by default when traffic crosses between the other interfaces.

You can create multiple NAT policies on a SonicWALL running SonicOS Enhanced for the same object – for instance, you can specify that an internal server uses one IP address when accessing Telnet servers, and uses a different IP address for all other protocols. Because the NAT engine in SonicOS Enhanced supports inbound port forwarding, it is possible to access multiple internal servers from the WAN IP address of the SonicWALL security appliance. The more granular the NAT Policy, the more precedence it takes.

Before configuring NAT Policies, you must create all Address Objects that will be referenced by the policy. For instance, if you are creating a One-to-One NAT policy, first create Address Objects for your public and private IP addresses.

Address Objects are one of four object classes (Address, User, Service, and Schedule) in SonicOS Enhanced. Once you define an Address Object, it becomes available for use wherever applicable throughout the SonicOS management interface. For example, consider an internal Web server with an IP address of 67.115.118.80. Rather than repeatedly typing in the IP address when constructing Access Rules or NAT Policies, you can create an Address Object to store the Web server's IP address. This Address Object, "My Web Server," can then be used in any configuration screen that employs Address Objects as a defining criterion.

Since there are multiple types of network address expressions, there are currently the following Address Objects types:

- **Host –** Host Address Objects define a single host by its IP address.
- **Range –** Range Address Objects define a range of contiguous IP addresses.
- **Network –** Network Address Objects are like Range objects in that they comprise multiple hosts, but rather than being bound by specified upper and lower range delimiters, the boundaries are defined by a valid netmask.
- **MAC Address –** MAC Address Objects allow for the identification of a host by its hardware address or MAC (Media Access Control) address.
- **FQDN Address –** FQDN Address Objects allow for the identification of a host by its Fully Qualified Domain Names (FQDN), such as www.sonicwall.com.

SonicOS Enhanced provides a number of default Address Objects that cannot be modified or deleted. You can use the default Address Objects when creating a NAT policy, or you can create custom Address Objects to use. All Address Objects are available in the drop-down lists when creating a NAT policy.

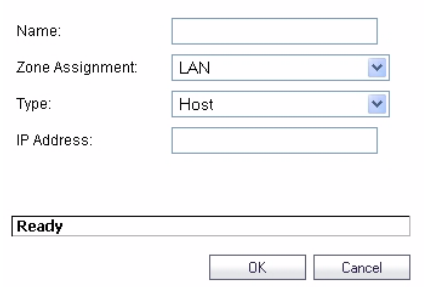
Creating Address Objects

The **Network** > **Address Objects** page allows you to create and manage your Address Objects. You can view Address Objects in the following ways using the **View Style** menu:

- **All Address Objects** – displays all configured Address Objects.
- **Custom Address Objects** – displays Address Objects with custom properties.
- **Default Address Objects** – displays Address Objects configured by default on the SonicWALL security appliance.

To add an Address Object:

1. Navigate to the **Network** > **Address Objects** page.
2. Below the **Address Objects** table, click **Add**.
3. In the **Add Address Object** dialog box, enter a name for the Address Object in the **Name** field.



4. Select the zone to assign to the Address Object from the **Zone Assignment** drop-down list.
5. Select **Host**, **Range**, **Network**, **MAC**, or **FQDN** from the **Type** menu.
   - For **Host**, enter the IP address in the **IP Address** field.
   - For **Range**, enter the starting and ending IP addresses in the **Starting IP Address** and **Ending IP Address** fields.
   - For **Network**, enter the network IP address and netmask in the **Network** and **Netmask** fields.
   - For **MAC**, enter the MAC address in the **MAC Address** field.
   - For **FQDN**, enter the domain name for the individual site or range of sites (with a wildcard) in the **FQDN** field.
6. Click **OK**.

Configuring NAT Policies

NAT policies allow you to control Network Address Translation based on matching combinations of Source IP address, Destination IP address and Destination Services. Policy-based NAT allows you to deploy different types of NAT simultaneously. The following NAT configurations are available in SonicOS Enhanced:

- Many-to-One NAT Policy
- Many-to-Many NAT Policy
- One-to-One NAT Policy for Outbound Traffic
- One-to-One NAT Policy for Inbound Traffic (Reflexive)
- One-to-Many NAT Load Balancing
- Inbound Port Address Translation via One-to-One NAT Policy
- Inbound Port Address Translation via WAN IP Address

This section describes how to configure a One-to-One NAT policy. One-to-One is the most common NAT policy used to route traffic to an internal server, such as a Web server. Most of the time, this means that incoming requests from external IPs are translated from the IP address of the SonicWALL security appliance WAN port to the IP address of the internal Web server. An example configuration illustrates the use of the fields in the Add NAT Policy procedure. To add a One-to-One NAT policy that allows all Internet traffic to be routed through a public IP address, two policies are needed: one for the outbound traffic, and one for the inbound traffic.

To add the components of a One-to-One NAT policy, perform the following steps:

1. Navigate to the **Network** > **NAT Policies** page. Click **Add**. The **Add NAT Policy** dialog box displays.
2. For **Original Source**, select **Any**.
3. For **Translated Source**, select **Original**.
4. For **Original Destination**, select **X0 IP**.
5. For **Translated Destination**, select **Create new address object** and create a new address object using **WAN** for Zone Assignment and **Host** for Type.
6. For **Original Service**, select **HTTP**.
7. For **Translated Service,** select **Original**.
8. For **Inbound Interface**, select **X0**.
9. For **Outbound Interface**, select **Any**.
10. For **Comment**, enter a short description.
11. Select the **Enable NAT Policy** checkbox.
12. Select the **Create a reflexive policy** checkbox if you want a matching NAT Policy to be automatically created in the opposite direction. This will create the outbound as well as the inbound policies.
13. Click **Add**.

Policies for subnets behind the other interfaces of the SonicWALL security appliance can be created by emulating these steps. Create a new NAT policy in which you adjust the source interface and specify the **Original Source**: the subnet behind that interface.

Upgrading Firmware on Your SonicWALL

- *Obtaining the Latest Firmware* - page 58
- *Saving a Backup Copy of Your Preferences* - page 58
- *Upgrading the Firmware with Current Settings* - page 59
- *Using SafeMode to Upgrade Firmware* - page 59

Obtaining the Latest Firmware

1. To obtain a new SonicOS Enhanced firmware image file for your SonicWALL security appliance, connect to your MySonicWALL account at: <http://www.mysonicwall.com>
2. Copy the new SonicOS Enhanced image file to a convenient location on your management station.

Saving a Backup Copy of Your Preferences

Before beginning the update process, make a system backup of your SonicWALL security appliance configuration settings. The backup feature saves a copy of the current configuration settings on your SonicWALL security appliance, protecting all your existing settings in the event that it becomes necessary to return to a previous configuration state. The System Backup shows you the current configuration and firmware in a single, clickable restore image.

In addition to using the backup feature to save your current configuration state to the SonicWALL security appliance, you can export the configuration preferences file to a directory on your local management station. This file serves as an external backup of the configuration preferences, and can be imported back into the SonicWALL security appliance.

Perform the following procedures to save a backup of your configuration settings and export them to a file on your local management station:

1. On the **System** > **Settings** page, click **Create Backup**. Your configuration preferences are saved. The System Backup entry is displayed in the **Firmware Management** table.
2. To export your settings to a local file, click **Export Settings**. A popup window displays the name of the saved file.

Upgrading the Firmware with Current Settings

Perform the following steps to upload new firmware to your SonicWALL appliance and use your current configuration settings upon startup.

The appliance must be properly registered before it can be upgraded. Refer to *Registering and Licensing Your Appliance on MySonicWALL - page 13* for more information.

1. Download the SonicOS Enhanced firmware image file from MySonicWALL and save it to a location on your local computer.
2. On the **System** > **Settings** page, click **Upload New Firmware**.
3. Browse to the location where you saved the SonicOS Enhanced firmware image file, select the file and click the **Upload** button.
4. On the **System** > **Settings** page, click the **Boot** icon in the row for **Uploaded Firmware**.

Note: On the **System** > **Settings** page, click the **Boot** icon in the row for **Uploaded Firmware with Factory Default Settings**.

5. In the confirmation dialog box, click **OK**. The SonicWALL restarts and then displays the login page.
6. Enter your user name and password. Your new SonicOS Enhanced image version information is listed on the **System** > **Settings** page.

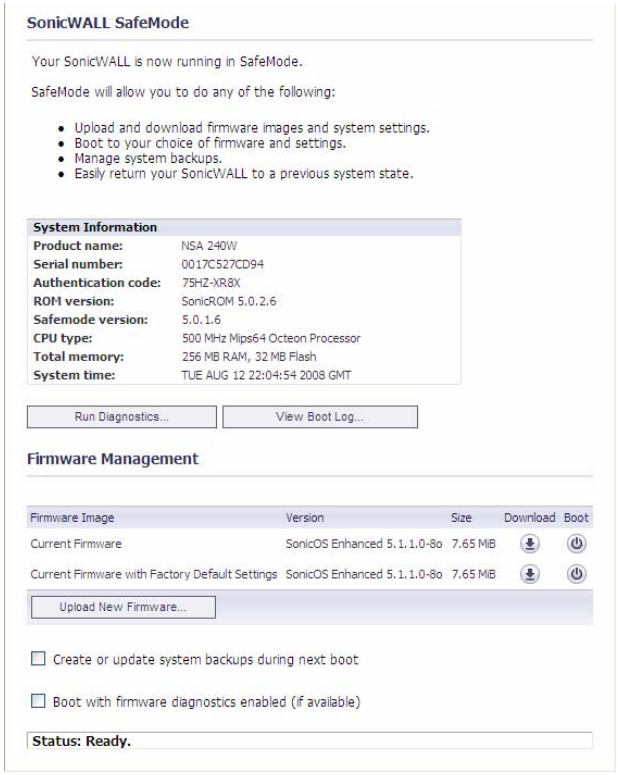
Using SafeMode to Upgrade Firmware

If you are unable to connect to the SonicWALL security appliance's management interface, you can restart the SonicWALL security appliance in SafeMode. The SafeMode feature allows you to recover quickly from uncertain configuration states with a simplified management interface that includes the same settings available on the **System** > **Settings** page.

To use SafeMode to upgrade firmware on the SonicWALL security appliance, perform the following steps:

1. Connect your computer to the X0 port on the SonicWALL appliance and configure your IP address with an address on the 192.168.168.0/24 subnet, such as 192.168.168.20.
2. To configure the appliance in SafeMode, perform one of the following:
   - Use a narrow, straight object, like a straightened paper clip or a toothpick, to press and hold the reset button on the back of the security appliance for one second. The reset button is in a small hole next to the power supply.
   - The Test light starts blinking when the SonicWALL security appliance has rebooted into SafeMode.

3. Point the Web browser on your computer to **192.168.168.168**. The SafeMode management interface displays.


SonicWALL SafeMode
Your SonicWALL is now running in SafeMode.
SafeMode will allow you to do any of the following:
Upload and download firmware images and system settings.
Boot to your choice of firmware and settings.
Manage system backups.
Easily return your SonicWALL to a previous system state.
System Information
Product name: NSA 240W
Serial number: 0017C527CD94
Authentication code: 75HZ-XR8X
ROM version: SonicROM 5.0.2.6
Safemode version: 5.0.1.6
CPU type: 500 MHz Mips64 Octeon Processor
Total memory: 256 MB RAM, 32 MB Flash
System time: TUE AUG 12 22:04:54 2008 GMT
Run Diagnostics...
View Boot Log...
Firmware Management
Firmware Image
Version
Size
Download
Boot
Current Firmware
SonicOS Enhanced 5.1.1.0-8o
7.65 MiB
Current Firmware with Factory Default Settings
SonicOS Enhanced 5.1.1.0-8o
7.65 MiB
Upload New Firmware...
Create or update system backups during next boot
Boot with firmware diagnostics enabled (if available)
Status: Ready.

4. If you have made any configuration changes to the security appliance, select the **Create Backup On Next Boot** checkbox to make a backup copy of your current settings. Your settings will be saved when the appliance restarts.
5. Click **Upload New Firmware**, and then browse to the location where you saved the SonicOS Enhanced firmware image, select the file and click the **Upload** button.
6. Select the boot icon in the row for one of the following:
   - **Uploaded Firmware - New!**
     Use this option to restart the appliance with your current configuration settings.
   - **Uploaded Firmware with Factory Defaults - New!**
     Use this option to restart the appliance with default configuration settings.
7. In the confirmation dialog box, click **OK** to proceed.
8. After successfully booting the firmware, the login screen is displayed. If you booted with factory default settings, enter the default user name and password (admin / password) to access the SonicWALL management interface.

Note: *Remember to change your IP address settings back to DHCP. Otherwise, you may not be able to connect to the Internet.*

Deploying SonicPoints for Wireless Access

This section describes how to configure SonicPoints with the SonicWALL NSA 240. See the following subsections:

- *Updating SonicPoint Firmware - page 61*
- *Configuring SonicPoint Provisioning Profiles - page 61*
- *Configuring a Wireless Zone - page 63*
- *Assigning an Interface to the Wireless Zone - page 64*
- *Connecting the SonicPoint - page 65*

SonicWALL SonicPoints are wireless access points specially engineered to work with SonicWALL security appliances to provide wireless access throughout your enterprise. The SonicPoint section of the SonicOS management interface lets you manage the SonicPoints connected to your system.

Before you can manage SonicPoints in the Management Interface, you must first:

- Verify that the SonicPoint image is downloaded to your SonicWALL security appliance.
- Configure your SonicPoint provisioning profiles.
- Configure a Wireless zone.
- Assign profiles to wireless zones. This step is optional. If you do not assign a default profile for a zone, SonicPoints in that zone will use the first profile in the list.
- Assign an interface to the Wireless zone.
- Attach the SonicPoints to the interface in the Wireless zone and test.

Updating SonicPoint Firmware

If your SonicWALL appliance has Internet connectivity, it will automatically download the correct version of the SonicPoint when you connect a SonicPoint device. See the *SonicOS Enhanced Administrator's Guide* for more details.

Configuring SonicPoint Provisioning Profiles

SonicPoint Profile definitions include all of the settings that can be configured on a SonicPoint, such as radio settings for the 2.4GHz and 5GHz radios, SSIDs and channels of operation.

Once you have defined a SonicPoint profile, you can apply it to a Wireless zone. Each Wireless zone can be configured with one SonicPoint profile. When a SonicPoint is connected to a zone, it is automatically provisioned with the profile assigned to that zone. SonicOS includes a default SonicPoint profile, named SonicPoint.

To add a new profile, click **Add** below the list of SonicPoint provisioning profiles. To edit an existing profile, select the profile and click the **Configure** icon in the same line as the profile you are editing.

1. In the Add/Edit SonicPoint Profile window on the **General** tab:
   - Select **Enable SonicPoint**.
   - Enter a **Name Prefix** to be used as the first part of the name for each SonicPoint provisioned.
   - Select the **Country Code** for where the SonicPoints are operating.

2. In the **802.11g Radio** tab:
   - Select **Enable Radio**.
   - Select a schedule for the radio to be enabled from the drop-down list.
   - For **Radio Mode**, select the speed that the SonicPoint will operate on. You can choose from the following:
     - 11Mbps - 802.11b
     - 54 Mbps - 802.11g
     - 108 Mbps - Turbo G

Note: *If you choose Turbo mode, all users in your company must use wireless access cards that support Turbo mode.*

   - For **Channel**, use AutoChannel unless you have a reason to use or avoid specific channels.
   - Enter a recognizable string for the **SSID** of each SonicPoint using this profile. This is the name that will appear in clients' lists of available wireless connections.
   - Under **ACL Enforcement**, select **Enable MAC Filter List** to enforce Access Control by allowing or denying traffic from specific devices. Select a MAC address object group from the **Allow List** to automatically allow traffic from all devices with MAC addresses in the group. Select a MAC address group from the **Deny List** to automatically deny traffic from all devices with MAC addresses in the group. The Deny List is enforced before the Allow List.
   - Under **WEP/WPA Encryption**, select the **Authentication Type** for your wireless network. SonicWALL recommends using **WPA2** as the authentication type.

Note: *WPA2 is a more secure replacement for the older WEP and WPA standards.*

   - Fill in the fields specific to the authentication type that you selected. The remaining fields change depending on the selected authentication type.
3. In the **802.11g Adv** tab, configure the advanced radio settings for the 802.11g radio. For most 802.11g advanced options, the default settings give optimum performance. For a full description of the fields on this tab, see the *SonicOS Enhanced Administrator's Guide*.
4. In the **802.11a Radio** and **802.11a Adv** tabs, configure the settings for the operation of the 802.11a radio bands. The SonicPoint has two separate radios built in. Therefore, it can send and receive on both the 802.11a and 802.11g bands at the same time.
   The settings in the **802.11a Radio** and **802.11a Advanced** tabs are similar to the settings in the **802.11g Radio** and **802.11g Advanced** tabs.
5. When finished, click **OK**.

Configuring a Wireless Zone

You can configure a wireless zone on the **Network** > **Zones** page. Typically, you will configure the WLAN zone for use with SonicPoints.

1. On the **Network** > **Zones** page in the **WLAN** row, click the icon in the **Configure** column.
2. In the Edit Zone dialog box on the **General** tab, the **Allow Interface Trust** setting automates the creation of Access Rules to allow traffic to flow between the interfaces of a zone instance. For example, if the WLAN Zone has both the **X2** and **X3** interfaces assigned to it, checking **Allow Interface Trust** on the WLAN Zone creates the necessary Access Rules to allow hosts on these interfaces to communicate with each other.
3. Select the checkboxes for the security services to enable on this zone. Typically you would enable **Gateway Anti-Virus**, **IPS**, and **Anti-Spyware**. If your wireless clients are all running SonicWALL Client Anti-Virus, select **Enable Client AV Enforcement Service**.
4. Click the **Wireless** tab.
   - In the **Wireless Settings** section, select **Only allow traffic generated by a SonicPoint** to allow only traffic from SonicWALL SonicPoints to enter the WLAN Zone interface. This provides maximum security on your WLAN. Uncheck this option if you want to allow any traffic on your WLAN Zone regardless of whether or not it is from a SonicPoint.
   - Select **SSL VPN Enforcement** to require that all traffic that enters into the WLAN Zone be authenticated through a SonicWALL SSL VPN appliance.

Tip: *For two-factor user authentication, SSL VPN Enforcement allows the added security of one-time passwords when using a SonicWALL SSL VPN appliance.*

   - In the **SSL VPN Server** list, select an address object to direct traffic to the SonicWALL SSL VPN appliance.
   - In the **SSL VPN Service** list, select the service or group of services that you want to allow for clients authenticated through the SSL VPN.
   - If your wireless network is already running WiFiSec, you can select **WiFiSec Enforcement** to require that all traffic that enters into the WLAN Zone interface be either IPsec traffic, WPA traffic, or both. If you have configured WPA2 as your authentication type, you do not need to enable WiFiSec.

If you have enabled **WiFiSec Enforcement**, you can specify the following:

- Select **WiFiSec Exception Service** to select services that are allowed to bypass the WiFiSec enforcement.
- Select **Require WiFiSec for Site-to-Site VPN Tunnel Traversal** to require WiFiSec security for all wireless connections through the WLAN zone that are part of a Site-to-Site VPN.
- If you wish to run WPA or WPA2 in addition to WiFiSec, you can select **Trust WPA/WPA2 traffic as WiFiSec** to accept WPA and WPA2 as allowable alternatives to WiFiSec.
- Under **SonicPoint Settings**, select the **SonicPoint Provisioning Profile** you want to apply to all SonicPoints connected to this zone. Whenever a SonicPoint connects to this zone, it will automatically be provisioned by the settings in the SonicPoint Provisioning Profile, unless you have individually configured it with different settings.

5. Optionally configure the settings on the **Guest Services** tab. For information about configuring Guest Services, see the *SonicOS Enhanced Administrator's Guide*.
6. When finished, click **OK**.

Assigning an Interface to the Wireless Zone

Once the wireless zone is configured, you can assign an interface to it. This is the interface where you will connect the SonicPoint.

1. On the **Network** > **Interfaces** page, click the **Configure** icon in the row for the interface that you want to use, for example, X3. The interface must be unassigned.
2. In the Edit Interface dialog box on the **General** tab, select **WLAN** or the zone that you created from the **Zone** drop-down list. Additional fields are displayed.
3. Enter the IP address and subnet mask of the Zone in the **IP Address** and **Subnet Mask** fields.
4. In the **SonicPoint Limit** field, select the maximum number of SonicPoints allowed on this interface.
5. If you want to enable remote management of the SonicWALL security appliance from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **SSH**, **Ping**, **SNMP**, and/or **SSH**.
6. If you want to allow selected users with limited management rights to log in to the security appliance, select **HTTP** and/or **HTTPS** in **User Login**.
7. Click **OK**.

Connecting the SonicPoint

When a SonicPoint unit is first connected and powered up, it will have a factory default configuration (IP Address 192.168.1.20, username: **admin**, password: **password**). Upon initializing, it will attempt to find a SonicOS device with which to peer. If it is unable to find a peer SonicOS device, it will enter into a stand-alone mode of operation with a separate stand-alone configuration allowing it to operate as a standard Access Point.

If the SonicPoint locates a peer SonicOS device via the SonicWALL Discovery Protocol, the two units perform an encrypted exchange and the profile assigned to the relevant wireless zone is used to automatically configure (provision) the newly added SonicPoint unit.

As part of the provisioning process, SonicOS assigns the discovered SonicPoint device a unique name, records the SonicPoint's MAC address and the interface and zone on which it was discovered, and uses the profile associated with the relevant zone to configure the 2.4GHz and 5GHz radio settings. It can also automatically assign the SonicPoint an IP address, if so configured, so that the SonicPoint can communicate with an authentication server for WPA-EAP support.

To connect the SonicPoint:

1. Using a CAT 5 Ethernet cable, connect the SonicPoint to the interface that you configured. Then connect the SonicPoint to a power source.
2. In the SonicOS user interface on the **SonicPoint** > **SonicPoints** page, click the **Synchronize SonicPoints** button. The SonicWALL appliance downloads a SonicPoint image from the SonicWALL back-end server.
3. Follow the instructions in the SonicPoint wizard. Be sure to select the same authentication type and enter the same keys or password that you configured in SonicOS.

For more information about wireless configuration, see the *SonicOS Enhanced Administrator's Guide*.

Troubleshooting Diagnostic Tools

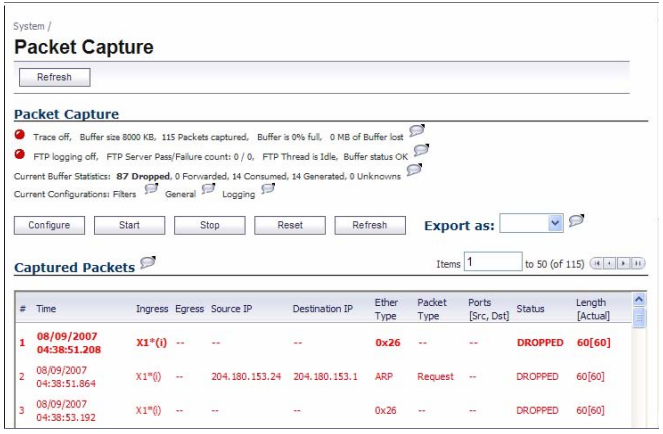
SonicOS provides a number of diagnostic tools to help you maintain your network and troubleshoot problems. Several tools can be accessed on the **System** > **Diagnostics** page, and others are available on other screens.

This section contains the following subsections:

- *Using Packet Capture* - page 66
- *Using Ping* - page 68
- *Using the Active Connections Monitor* - page 68
- *Using the Log > View Page* - page 69

Using Packet Capture

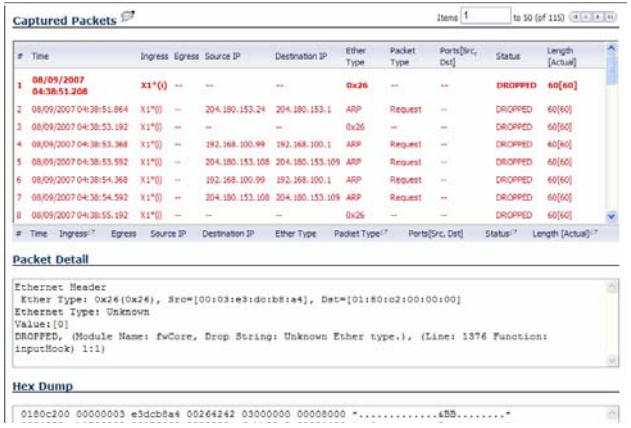
Packet Capture allows you to capture and examine the contents of individual data packets that traverse your SonicWALL firewall appliance. The captured packets contain both data and addressing information. The **System** > **Packet Capture** page provides a way to configure the capture criteria, display settings and file export settings, and displays the captured packets.


System /
Packet Capture
Refresh
Packet Capture
Trace off, Buffer size 8000 KB, 115 Packets captured, Buffer is 0% full, 0 MB of Buffer lost
FTP logging off, FTP Server Pass/Failure count: 0 / 0, FTP Thread is Idle, Buffer status OK
Current Buffer Statistics: 87 Dropped, 0 Forwarded, 14 Consumed, 14 Generated, 0 Unknowns
Current Configurations: Filters General Logging
Configure
Start
Stop
Reset
Refresh
Export as:
Captured Packets
Items 1 to 50 (of 115)
Time Ingress Egress Source IP Destination IP Ether Type Packet Type Ports [Src, Dst] Status Length [Actual]
1 08/09/2007 04:38:51.208 X1*(i) -- -- -- 0x26 -- -- DROPPED 60[60]
2 08/09/2007 04:38:51.864 X1*(i) -- 204.180.153.24 204.180.153.1 ARP Request -- DROPPED 60[60]
3 08/09/2007 04:38:53.192 X1*(i) -- -- -- 0x26 -- -- DROPPED 60[60]

The Packet Capture screen has buttons for starting and stopping a packet capture. If you simply click **Start** without any configuration, the SonicWALL appliance will capture all packets except those for internal communication, and will stop when the buffer is full or when you click **Stop**.

The SonicOS user interface provides three windows to display different views of the captured packets:

- Captured Packets
- Packet Detail
- Hex Dump

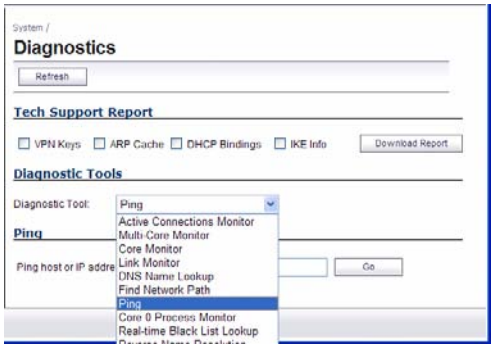

Captured Packets
Items 1 to 50 (of 115)
Time Ingress Egress Source IP Destination IP Ether Type Packet Type Ports[Src, Dst] Status Length [Actual]
1 08/09/2007 04:38:51.208 X1*(i) -- -- -- 0x26 -- -- DROPPED 60[60]
2 08/09/2007 04:38:51.864 X1*(i) -- 204.180.153.24 204.180.153.1 ARP Request -- DROPPED 60[60]
3 08/09/2007 04:38:53.192 X1*(i) -- -- -- 0x26 -- -- DROPPED 60[60]
4 08/09/2007 04:38:53.368 X1*(i) -- 192.168.100.99 192.168.100.1 ARP Request -- DROPPED 60[60]
5 08/09/2007 04:38:53.592 X1*(i) -- 204.180.153.108 204.180.153.109 ARP Request -- DROPPED 60[60]
6 08/09/2007 04:38:54.368 X1*(i) -- 192.168.100.99 192.168.100.1 ARP Request -- DROPPED 60[60]
7 08/09/2007 04:38:54.592 X1*(i) -- 204.180.153.108 204.180.153.109 ARP Request -- DROPPED 60[60]
8 08/09/2007 04:38:55.192 X1*(i) -- -- -- 0x26 -- -- DROPPED 60[60]
Time Ingress Egress Source IP Destination IP Ether Type Packet Type Ports[Src, Dst] Status Length [Actual]
Packet Detail
Ethernet Header
Ether Type: 0x26(0x26), Src=[00:03:e3:dc:b8:a4], Dst=[01:80:c2:00:00:00]
Ethernet Type: Unknown
Value:[0]
DROPPED, (Module Name: fwCore, Drop String: Unknown Ether type.), (Line: 1376 Function: inputHook) 1:1)
Hex Dump
0180c200 00000003 e3dcb8a4 00264242 03000000 00008000 "..............&BB........"

Click the **Configure** button to customize the settings for the capture. Once the configuration is complete, click **Start** to begin capturing packets. The settings available in the five main areas of configuration are summarized below:

- **General** – number of bytes to capture, wrap capture buffer
- **Capture Filter** – interfaces, packet types, source/ destination
- **Display Filter** – interfaces, packet types, source/ destination
- **Logging** – automatic transfer of buffer to FTP server
- **Advanced** – generated packets, SonicWALL GMS, syslog, management

Using Ping

Ping is available on the **System** > **Diagnostics** page.

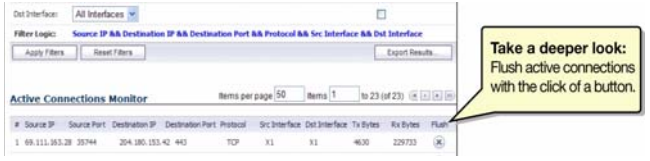


The Ping test bounces a packet off a machine on the Internet and returns it to the sender. This test shows if the SonicWALL security appliance is able to contact the remote host. If users on the LAN are having problems accessing services on the Internet, try pinging the DNS server, or another machine at the ISP location. If the test is unsuccessful, try pinging devices outside the ISP. If you can ping devices outside of the ISP, then the problem lies with the ISP connection.

Using the Active Connections Monitor

The **Active Connections Monitor** displays real-time, exportable (plain text or CSV), filterable views of all connections to and through the SonicWALL security appliance. This tool is available on the **Systems** > **Diagnostics** page.

You can filter the results to display only connections matching certain criteria. You can filter by **Source IP**, **Destination IP**, **Destination Port**, **Protocol**, **Src Interface**, and **DST Interface**. Enter your filter criteria in the **Active Connections Monitor Settings** table. The fields you enter values into are combined into a search string with a logical **AND**. Select the **Group Filters** box next to any two or more criteria to combine them with a logical **OR**.

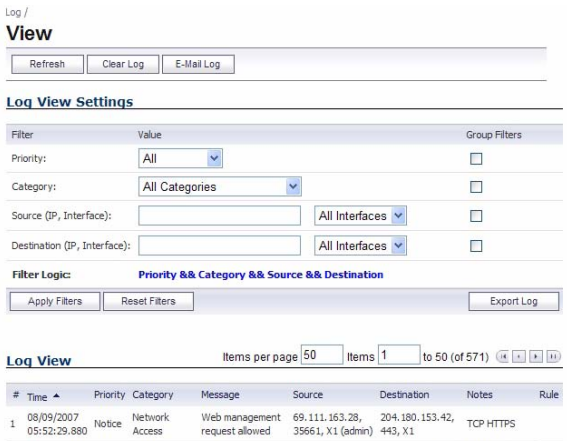


Using the Log > View Page

The SonicWALL security appliance maintains an Event log for tracking potential security threats. You can view the log in the **Log** > **View** page, or it can be automatically sent to an email address for convenience and archiving. The log is displayed in a table and can be sorted by column.

You can filter the results to display only event logs matching certain criteria. You can filter by **Priority**, **Category**, **Source** (**IP** or **Interface**), and **Destination** (**IP** or **Interface**).

The fields you enter values into are combined into a search string with a logical **AND**. Select the **Group Filters** box next to any two or more criteria to combine them with a logical **OR**.



Deployment Configuration Reference Checklist

Use this checklist to find more information about various deployment tasks within the *SonicOS Enhanced Administrator's Guide*.

For this Task...	See this Chapter...
Inspecting the rule base for inbound and outbound rules	Configuring Access Rules
Setting logging levels	Configuring Log Categories ("Logging Level" section)
Configuring threat prevention on all used zones	Configuring Zones ("Enabling SonicWALL Security Services on Zones" section)
Configuring Web filtering protection	Configuring SonicWALL Content Filtering Service
Changing administrator login	Configuring Administration Settings ("Administrator Name & Password" section)
Setting administrator email	Configuring Log Automation ("Email Log Automation" section)
Disabling HTTP and ping access	Configuring Interfaces ("Configuring Advanced Settings for the Interfaces" section)
Disabling or enabling DHCP	Setting Up the DHCP Server
Configuring user management	Managing Users and Authentication Settings
Configuring VPN policies	Configuring VPN Policies
Securing wireless access	Managing SonicPoints

Support and Training Options 8

In this Section:

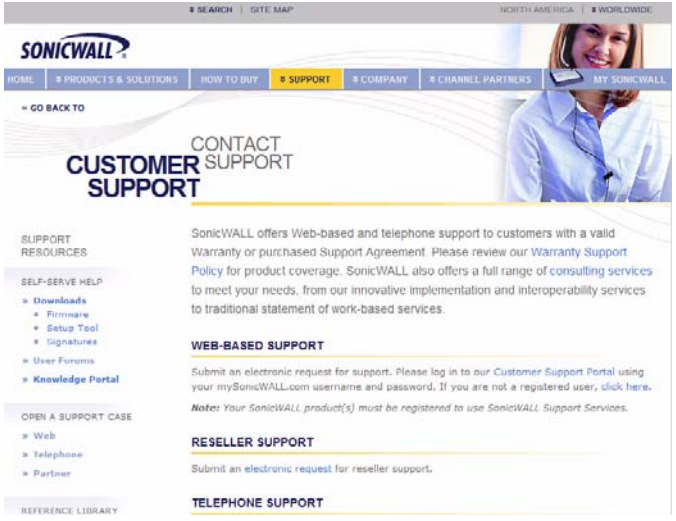
This section provides overviews of customer support and training options for the SonicWALL NSA 240.

- *Customer Support - page 72*
- *SonicWALL Live Product Demos - page 72*
- *Knowledge Portal - page 73*
- *Onboard Help - page 73*
- *User Forums - page 74*
- *Training - page 75*
- *Related Documentation - page 76*
- *SonicWALL Secure Wireless Network Integrated Solutions Guide - page 77*

Customer Support

SonicWALL offers Web-based and telephone support to customers who have a valid Warranty or who purchased a Support Contract. Please review our Warranty Support Policy for product coverage. SonicWALL also offers a full range of consulting services to meet your needs, from our innovative implementation services to traditional statement of work-based services.

For further information, visit:
<http://www.sonicwall.com/us/support/contact.html>

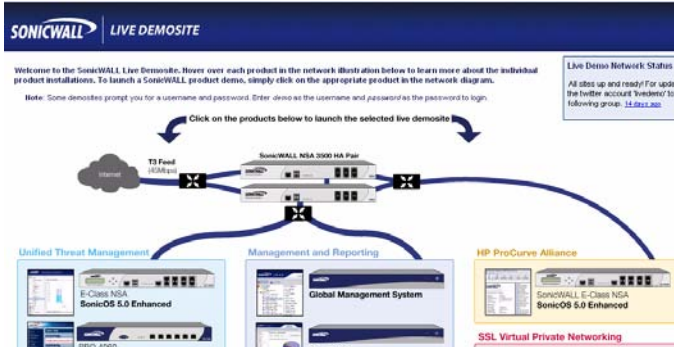

SEARCH | SITE MAP
NORTH AMERICA | WORLDWIDE
SONICWALL
HOME | PRODUCTS & SOLUTIONS | HOW TO BUY | SUPPORT | COMPANY | CHANNEL PARTNERS | MY SONICWALL
GO BACK TO
CONTACT
CUSTOMER SUPPORT
SUPPORT RESOURCES
SELF-SERVE HELP
Downloads
Firmware
Setup Tool
Signatures
User Forums
Knowledge Portal
OPEN A SUPPORT CASE
Web
Telephone
Partner
REFERENCE LIBRARY
SonicWALL offers Web-based and telephone support to customers with a valid Warranty or purchased Support Agreement. Please review our Warranty Support Policy for product coverage. SonicWALL also offers a full range of consulting services to meet your needs, from our innovative implementation and interoperability services to traditional statement of work-based services.
WEB-BASED SUPPORT
Submit an electronic request for support. Please log in to our Customer Support Portal using your mySonicWALL.com username and password. If you are not a registered user, click here.
Note: Your SonicWALL product(s) must be registered to use SonicWALL Support Services.
RESELLER SUPPORT
Submit an electronic request for reseller support.
TELEPHONE SUPPORT

SonicWALL Live Product Demos

The SonicWALL Live Demo Site provides free test drives of SonicWALL security products and services through interactive live product installations:

- Unified Threat Management Platform
- Secure Cellular Wireless
- Continuous Data Protection
- SSL VPN Secure Remote Access
- Content Filtering
- Secure Wireless Solutions
- Email Security
- SonicWALL GMS and ViewPoint

For further information, visit:
<http://livedemo.sonicwall.com/>


SONICWALL LIVE DEMOSITE
Welcome to the SonicWALL Live Demosite. Hover over each product in the network illustration below to learn more about the individual product installations. To launch a SonicWALL product demo, simply click on the appropriate product in the network diagram.
Note: Some demosites prompt you for a username and password. Enter demo as the username and password as the password to login.
Live Demo Network Status
Click on the products below to launch the selected live demosite
Internet
T3 Feed
SonicWALL NSA 3500 HA Pair
Unified Threat Management
E-Class NSA
SonicOS 5.0 Enhanced
Management and Reporting
Global Management System
HP ProCurve Alliance
SonicWALL E-Class NSA
SonicOS 5.0 Enhanced
SSL Virtual Private Networking

Knowledge Portal

The Knowledge Portal allows users to search for SonicWALL documents based on the following types of search tools:

- Browse
- Search for keywords
- Full-text search

For further information, navigate to the **Support** > **Knowledge Portal** page at:
<http://www.mysonicwall.com/>

SONICWALL
Home
Q&A Search
Ask A Question
My Profile
My Alerts
SonicWALL Customer Support Knowledge Portal
Welcome!
We're happy to see you here at the SonicWALL Customer Support Knowledge Portal! Please use one of the available subsections below to get started.
Find Answers
To start searching for articles within the Knowledge Portal, enter a query in the search box and press the Search button or select a category from the list below, and click Get Answers. From there, you can refine your search with specific keywords. You can also see a list of all available categories to further refine your search. Or, just enter a Knowledge Item's ID number in the field below and click Get Knowledge Item Number to see it.
Keywords:
Search
OR
Get Knowledge Item Number:
My SonicWALL Customer Support Knowledge Portal
Use the Bookmarks and Alerts button below to set and customize alerts for knowledge item updates!
Bookmarks and Alerts
Review the Top 25 Questions
Select a category below to see the top 25 knowledge items (questions) for that category.
– Search All Categories –
Get Top 25
What's New!
Aventail EX Series SSL VPN articles have been moved to the SSL VPN (Remote Access) category.
SSL-VPN firmware version 3.0 has recently been released.
SonicOS Enhanced 3.9.0.3 and SonicOS Standard 3.9.0.0 have been released for TZ 180, 180W (wireless), 190 and

Onboard Help

SonicOS features a dynamic Onboard Help in the form of helpful tooltips that appear over various elements of the GUI when the mouse hovers over them. Elements that display these tooltips include text fields, radio buttons, and checkboxes.

User Forums

The SonicWALL User Forums is a resource that provides users the ability to communicate and discuss a variety of security and appliance subject matters. In this forum, the following categories are available for users:

- Content Security Manager topics
- Continuous Data Protection topics
- Email Security topics
- Firewall topics
- Network Anti-Virus topics
- Security Services and Content Filtering topics
- SonicWALL GMS and Viewpoint topics
- SonicPoint and Wireless topics
- SSL VPN topics
- NSA 240 / Wireless WAN - 3G Capability topics
- VPN Client topics
- VPN site-to-site and interoperability topics

For further information, visit:
<https://forum.sonicwall.com/>

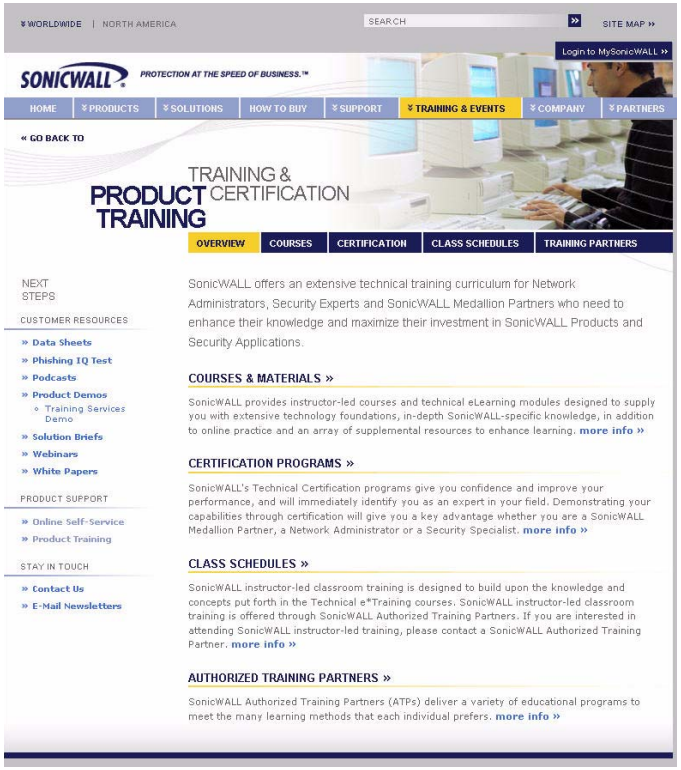
SONICWALL
Comprehensive Internet Security
SonicWALL Forums
Welcome, amendoza@sonicwall.com.
You last visited: 01-01-1970 at 12:00 AM
Private Messages: Unread 0, Total 0.
User CP FAQ Calendar New Posts Search Quick Links KnowledgePortal Log Out
Forum Last Post Threads Posts
Firewalls
Firewall related topics
Network
Networking related topics.
Multiple T-1's and Sonicwall... by tbeynon Today 10:56 PM 4,538 19,051
VPN
VPN site to site and interoperability topics
VPN client for MAC OSX adn... by mdominquez@marlinengineering.com Today 08:52 PM 1,973 6,800
VPN Client
VPN Client related topics
VPN Global CLient behind a... by mdominquez@marlinengineering.com Today 02:44 PM 1,795 8,366
SonicPoint / Wireless
SonicPoint and wireless related topics
IP Helper and DHCP on 2040... by jclement@chetm.com Today 08:26 PM 536 2,492
SGMS / Viewpoint
SGMS and Viewpoint related topics
Pls help--No syslog files... by indcenter Today 08:36 PM 756 2,650
Security Services
All IPS, Gateway Anti-Virus, Anti Spyware, Client AV, Application Firewall, and Content Filtering topics
AV and Spyware updates? by Huegel_admin Today 09:41 AM 1,062 4,316
Network Anti-Virus
Network Anti-Virus related topics
Network Antivirus Blocking... by templeiv@yahoo.com 07-20-2008 01:56 AM 225 1,028
TZ 190 / Wireless WAN
3G Capability on the new TZ 190
SonicOS Enhanced 3.9.0.1e... by jameswright72 Today 07:38 PM 113 461
Misc
Miscellaneous topics topics relating to SonicWALL firewalls
SOHO3 Upgrade to TZ180 by PAWELD Today 02:21 PM 1,112 4,047
SonicWALL SSL-VPN
SSL-VPN Topics
SSL-VPN 4000
SSL-VPN 4000 related topics
unsupported authentication... by johnt@alaskabillingservices.com Today 08:02 PM 58 253

Training

SonicWALL offers an extensive sales and technical training curriculum for Network Administrators, Security Experts and SonicWALL Medallion Partners who need to enhance their knowledge and maximize their investment in SonicWALL Products and Security Applications. SonicWALL Training provides the following resources for its customers:

- E-Training
- Instructor-Led Training
- Custom Training
- Technical Certification
- Authorized Training Partners

For further information, visit:
<http://www.sonicwall.com/us/support/training.html>

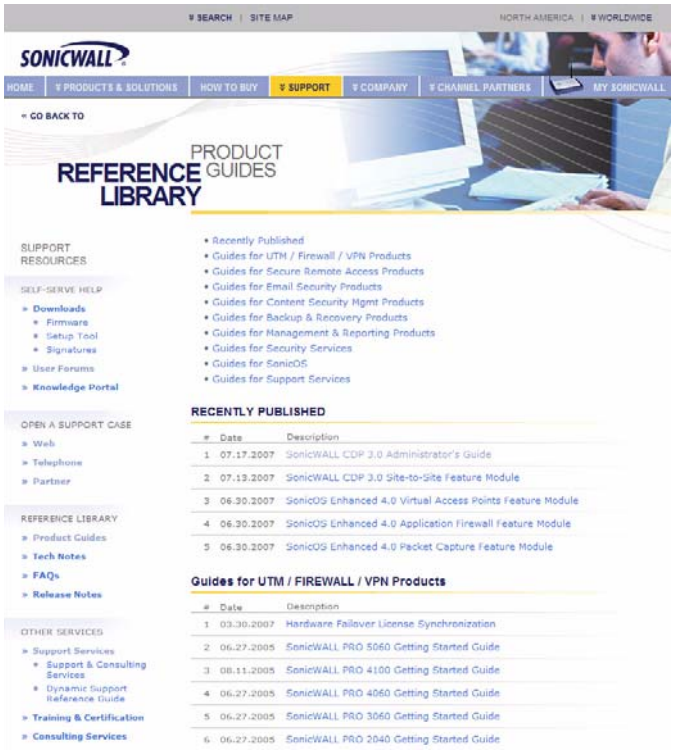

WORLDWIDE | NORTH AMERICA
SEARCH
SITE MAP »
Login to MySonicWALL »
SONICWALL
PROTECTION AT THE SPEED OF BUSINESS.™
HOME
PRODUCTS
SOLUTIONS
HOW TO BUY
SUPPORT
TRAINING & EVENTS
COMPANY
PARTNERS
« GO BACK TO
TRAINING &
PRODUCT CERTIFICATION
TRAINING
OVERVIEW
COURSES
CERTIFICATION
CLASS SCHEDULES
TRAINING PARTNERS
NEXT STEPS
CUSTOMER RESOURCES
» Data Sheets
» Phishing IQ Test
» Podcasts
» Product Demos
◦ Training Services Demo
» Solution Briefs
» Webinars
» White Papers
PRODUCT SUPPORT
» Online Self-Service
» Product Training
STAY IN TOUCH
» Contact Us
» E-Mail Newsletters
SonicWALL offers an extensive technical training curriculum for Network Administrators, Security Experts and SonicWALL Medallion Partners who need to enhance their knowledge and maximize their investment in SonicWALL Products and Security Applications.
COURSES & MATERIALS »
SonicWALL provides instructor-led courses and technical eLearning modules designed to supply you with extensive technology foundations, in-depth SonicWALL-specific knowledge, in addition to online practice and an array of supplemental resources to enhance learning. more info »
CERTIFICATION PROGRAMS »
SonicWALL's Technical Certification programs give you confidence and improve your performance, and will immediately identify you as an expert in your field. Demonstrating your capabilities through certification will give you a key advantage whether you are a SonicWALL Medallion Partner, a Network Administrator or a Security Specialist. more info »
CLASS SCHEDULES »
SonicWALL instructor-led classroom training is designed to build upon the knowledge and concepts put forth in the Technical e*Training courses. SonicWALL instructor-led classroom training is offered through SonicWALL Authorized Training Partners. If you are interested in attending SonicWALL instructor-led training, please contact a SonicWALL Authorized Training Partner. more info »
AUTHORIZED TRAINING PARTNERS »
SonicWALL Authorized Training Partners (ATPs) deliver a variety of educational programs to meet the many learning methods that each individual prefers. more info »

Related Documentation

See the following related documents for more information:

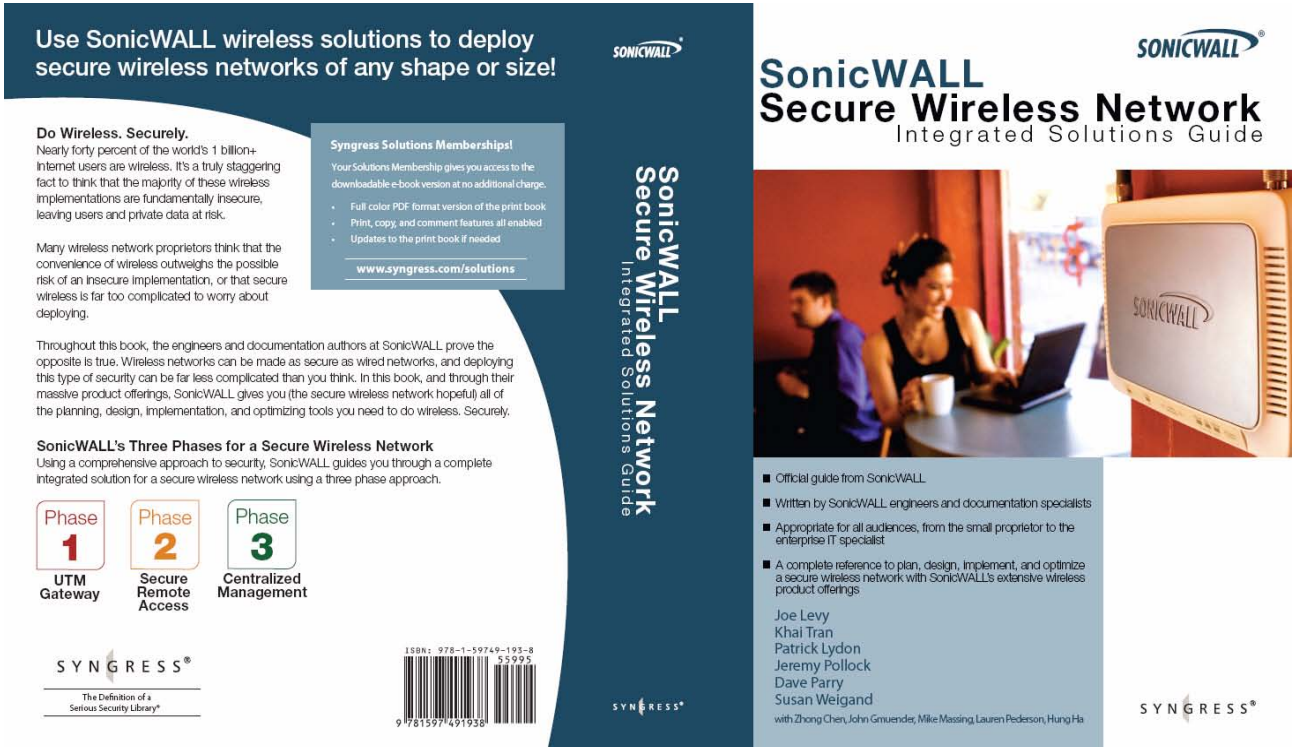
- *SonicOS Enhanced Administrator's Guide*
- *SonicOS Enhanced Release Notes*
- *SonicOS Enhanced Feature Modules*
  - Application Firewall
  - Dashboard
  - HA License Sync
  - Multiple Admin
  - NAT Load Balancing
  - Packet Capture
  - Radio Frequency Monitoring
  - Single Sign-On
  - SSL Control
  - Virtual Access Points
- *SonicWALL GMS 5.0 Administrator's Guide*
- *SonicWALL GVC 4.0 Administrator's Guide*
- *SonicWALL ViewPoint 5.0 Administrator's Guide*
- *SonicWALL GAV 4.0 Administrator's Guide*
- *SonicWALL IPS 2.0 Administrator's Guide*
- *SonicWALL Anti-Spyware Administrator's Guide*
- *SonicWALL CFS Administrator's Guide*

For further information, visit:
<http://www.sonicwall.com/us/support/289.html>


SEARCH | SITE MAP
NORTH AMERICA | WORLDWIDE
SONICWALL
HOME | PRODUCTS & SOLUTIONS | HOW TO BUY | SUPPORT | COMPANY | CHANNEL PARTNERS | MY SONICWALL
« GO BACK TO
PRODUCT
REFERENCE GUIDES
LIBRARY
SUPPORT RESOURCES
SELF-SERVE HELP
» Downloads
Firmware
Setup Tool
Signatures
» User Forums
» Knowledge Portal
OPEN A SUPPORT CASE
» Web
» Telephone
» Partner
REFERENCE LIBRARY
» Product Guides
» Tech Notes
» FAQs
» Release Notes
OTHER SERVICES
» Support Services
Support & Consulting Services
Dynamic Support Reference Guide
» Training & Certification
» Consulting Services
Recently Published
Guides for UTM / Firewall / VPN Products
Guides for Secure Remote Access Products
Guides for Email Security Products
Guides for Content Security Mgmt Products
Guides for Backup & Recovery Products
Guides for Management & Reporting Products
Guides for Security Services
Guides for SonicOS
Guides for Support Services
RECENTLY PUBLISHED
Date Description
1 07.17.2007 SonicWALL CDP 3.0 Administrator's Guide
2 07.13.2007 SonicWALL CDP 3.0 Site-to-Site Feature Module
3 06.30.2007 SonicOS Enhanced 4.0 Virtual Access Points Feature Module
4 06.30.2007 SonicOS Enhanced 4.0 Application Firewall Feature Module
5 06.30.2007 SonicOS Enhanced 4.0 Packet Capture Feature Module
Guides for UTM / FIREWALL / VPN Products
Date Description
1 03.30.2007 Hardware Failover License Synchronization
2 06.27.2005 SonicWALL PRO 5060 Getting Started Guide
3 08.11.2005 SonicWALL PRO 4100 Getting Started Guide
4 06.27.2005 SonicWALL PRO 4060 Getting Started Guide
5 06.27.2005 SonicWALL PRO 3060 Getting Started Guide
6 06.27.2005 SonicWALL PRO 2040 Getting Started Guide

SonicWALL Secure Wireless Network Integrated Solutions Guide

The Official Guide to SonicWALL's market-leading wireless networking and security devices. This 512-page book is available in hardcopy. Order the book directly from Elsevier Publishing at: <http://www.elsevier.com>


Use SonicWALL wireless solutions to deploy secure wireless networks of any shape or size!
SONICWALL
Do Wireless. Securely.
Nearly forty percent of the world's 1 billion+ Internet users are wireless. It's a truly staggering fact to think that the majority of these wireless implementations are fundamentally insecure, leaving users and private data at risk.
Many wireless network proprietors think that the convenience of wireless outweighs the possible risk of an insecure implementation, or that secure wireless is far too complicated to worry about deploying.
Syngress Solutions Memberships!
Your Solutions Membership gives you access to the downloadable e-book version at no additional charge.
Full color PDF format version of the print book
Print, copy, and comment features all enabled
Updates to the print book if needed
www.syngress.com/solutions
Throughout this book, the engineers and documentation authors at SonicWALL prove the opposite is true. Wireless networks can be made as secure as wired networks, and deploying this type of security can be far less complicated than you think. In this book, and through their massive product offerings, SonicWALL gives you (the secure wireless network hopeful) all of the planning, design, implementation, and optimizing tools you need to do wireless. Securely.
SonicWALL's Three Phases for a Secure Wireless Network
Using a comprehensive approach to security, SonicWALL guides you through a complete integrated solution for a secure wireless network using a three phase approach.
Phase 1 UTM Gateway
Phase 2 Secure Remote Access
Phase 3 Centralized Management
SYNGRESS®
The Definition of a Serious Security Library™
ISBN: 978-1-59749-193-8
55995
9 781597 491938
SonicWALL Secure Wireless Network Integrated Solutions Guide
SYNGRESS®
SONICWALL
SonicWALL Secure Wireless Network
Integrated Solutions Guide
Official guide from SonicWALL
Written by SonicWALL engineers and documentation specialists
Appropriate for all audiences, from the small proprietor to the enterprise IT specialist
A complete reference to plan, design, implement, and optimize a secure wireless network with SonicWALL's extensive wireless product offerings
Joe Levy
Khai Tran
Patrick Lydon
Jeremy Pollock
Dave Parry
Susan Weigand
with Zhong Chen, John Gmuender, Mike Massing, Lauren Pederson, Hung Ha
SYNGRESS®

Product Safety and Regulatory Information 9

In this Section:

This section provides regulatory, trademark, and copyright information.

- *Safety and Regulatory Information* - page 80
- *Safety and Regulatory Information in German* - page 81
- *FCC Part 15 Class A Notice* - page 82
- *Copyright Notice* - page 83
- *Trademarks* - page 83

Safety and Regulatory Information

Regulatory Model/Type	Product Name
APL19-05C	NSA 240

Mounting the SonicWALL

- Mount in a location away from direct sunlight and sources of heat. A maximum ambient temperature of 104º F (40º C) is recommended.
- Route cables away from power lines, fluorescent lighting fixtures, and sources of noise such as radios, transmitters, and broadband amplifiers
- The included power cord is intended for use in North America only. For European Union (EU) customers, a power cord is not included.
- Ensure that no water or excessive moisture can enter the unit.
- Allow unrestricted airflow around the unit and through the vents on the side of the unit. A minimum of 1 inch (25.44mm) clearance is recommended.
- Consideration must be given to the connection of the equipment to the supply circuit and the effect of over-loading the circuits has minimal impact on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings must be used when addressing this concern.

Lithium Battery Warning

The Lithium Battery used in the SonicWALL security appliance may not be replaced by the user. Return the SonicWALL security appliance to a SonicWALL-authorized service center for replacement with the same or equivalent type recommended by the manufacturer. If, for any reason, the battery or SonicWALL security appliance must be disposed of, do so following the battery manufacturer's instructions.

Cable Connections

All Ethernet and RS232 (Console) cables are designed for intra-building connection to other equipment. Do not connect these ports directly to communication wiring or other wiring that exits the building where the SonicWALL is located.

Power Supply Information

If the power supply is missing from your SonicWALL product package, please contact SonicWALL Technical Support at 408-752-7819 for a replacement. This product should only be used with a UL listed power supply marked “I.T.E. LPS”, with an output rated 12 VDC, minimum 3.0 A.

Safety and Regulatory Information in German

Weitere Hinweise zur Montage

- Wählen Sie für die Montage einen Ort, der keinem direkten Sonnenlicht ausgesetzt ist und sich nicht in der Nähe von Wärmequellen befindet. Die Umgebungstemperatur darf nicht mehr als 40 °C betragen.
- Achten Sie darauf, das sich die Netzwerkkabel nicht in der unmittelbaren Nähe von Stromleitungen, Leuchtstoffröhren und Störquellen wie Funksendern oder Breitbandverstärkern befinden.
- Das beigefügte Netzkabel ist nur für den Gebrauch in Nordamerikas Vorgesehen. Für Kunden in der Europaïschen Union (EU) ist ein Netzkabel nicht im Lieferumfang enthalten.
- Stellen Sie sicher, dass das Gerät vor Wasser und hoher Luftfeuchtigkeit geschützt ist.
- Stellen Sie sicher, dass die Luft um das Gerät herum zirkulieren kann und die Lüftungsschlitze an der Seite des Gehäuses frei sind. Hier ist ein Belüftungsabstand von mindestens 26 mm einzuhalten.
- Prüfen Sie den Anschluss des Geräts an die Stromversorgung, damit der Überstromschutz sowie die elektrische Leitung nicht von einer eventuellen Überlastung der Stromversorgung beeinflusst werden. Prüfen Sie dabei sorgfältig die Angaben auf dem Aufkleber des Geräts.

Hinweis zur Lithiumbatterie

Die in der Internet Security Appliance von SonicWALL verwendete Lithiumbatterie darf nicht vom Benutzer ausgetauscht werden. Zum Austauschen der Batterie muss die SonicWALL in ein von SonicWALL autorisiertes Service-Center gebracht werden. Dort wird die Batterie durch denselben oder entsprechenden, vom Hersteller empfohlenen Batterietyp ersetzt. Beachten Sie bei einer Entsorgung der Batterie oder der SonicWALL Internet Security Appliance die diesbezüglichen Anweisungen des Herstellers.

Kabelverbindungen

Alle Ethernet- und RS232-C-Kabel eignen sich für die Verbindung von Geräten in Innenräumen. Schließen Sie an die Anschlüsse der SonicWALL keine Kabel an, die aus dem Gebäude in dem sich das Gerät befindet, herausgeführt werden.

Informationen zur Stromversorgung

Wenn das Netzteil nicht im Lieferumfang des SonicWALL Produkts enthalten ist, wenden Sie sich bitte an den Technischen SonicWALL Support unter +1-408-752- 7819 für einen Ersatz. Dieses Produkt sollte nur mit einem UL-konformen Netzteil mit dem Logo "I.T.E. LPS" und einer Ausgangsleistung von12 VDC, Minimum 3,0 A.

FCC Part 15 Class A Notice

NOTE: This equipment was tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy. And if not installed and used in accordance with the instruction manual, the device may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user is required to correct the interference at his own expense.

Complies with EN 55022 Class A and CISPR22 Class A.

Warning: This is a class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Canadian Radio Frequency Emissions Statement

This Class A digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Declaration of Conformity

Application of council Directive	2004/108/EC (EMC) and 2006/95/EC (LVD)
Standards to which conformity is declared	EN 55022 (2006) Class A EN 55024 (1998) +A2 EN 61000-3-2 (2006) EN 61000-3-3 (1995) +A2 EN 60950-1 (2001) +A11 National Deviations: AT, AU, BE, CH, CN, CZ, DE, DK, FI, FR, GB, GR, HU, IE, IL, IN, IT, JP, KR, NL, NO, PL, SE, SG, SI

VCCI Statement

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－A

Caution: Modifying this equipment or using this equipment for purposes not shown in this manual without the written consent of SonicWALL, Inc. could void the user's authority to operate this equipment**.**

Regulatory Information for Korea

방송통신위원회	Ministry of Information and Telecommunication Certification Number "SWL-APL19-05C"

All products with country code “” (blank) and “A” are made in the USA.
All products with country code “B” are made in China.
All products with country code “C” or “D” are made in Taiwan R.O.C.
All certificates held by Secuwide, Corp.

A급 기기 (업무용 정보통신기기)

이 기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며, 만약 잘못판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Copyright Notice

© 2008-2010 SonicWALL, Inc.

All rights reserved.

Under the copyright laws, this manual or the software described within, cannot be copied, in whole or part, without the written consent of the manufacturer, except in the normal use of the software to make a backup copy. The same proprietary and copyright notices must be affixed to any permitted copies as were affixed to the original. This exception does not allow copies to be made for others, whether or not sold, but all of the material purchased (with all backup copies) can be sold, given, or loaned to another person. Under the law, copying includes translating into another language or format.

Specifications and descriptions subject to change without notice.

Trademarks

SonicWALL is a registered trademark of SonicWALL, Inc.

Microsoft Windows 98, Windows Vista, Windows 2000, Windows XP, Windows Server 2003, Internet Explorer, and Active Directory are trademarks or registered trademarks of Microsoft Corporation.

Netscape is a registered trademark of Netscape Communications Corporation in the U.S. and other countries. Netscape Navigator and Netscape Communicator are also trademarks of Netscape Communications Corporation and may be registered outside the U.S.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the U.S. and/or other countries.

Firefox is a trademark of the Mozilla Foundation.

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Notes

SonicWALL, Inc.

2001 Logic Drive
San Jose CA 95124-3452
www.sonicwall.com

T +1 408.745.9600
F +1 408.745.9300

P/N 232-001580-00
Rev A 2/2010

©2010 SonicWALL, Inc. is a registered trademark of SonicWALL, Inc. Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Specifications and descriptions subject to change without notice.